

A Class of Non-Linearly Solvable Networks *

Joseph Connelly and Kenneth Zeger

IEEE Transactions on Information Theory

Submitted: January 14, 2016

Abstract

For each integer $m \geq 2$, a network is constructed which is solvable over an alphabet of size m but is not solvable over any smaller alphabets. If m is composite, then the network has no vector linear solution over any R -module alphabet and is not asymptotically linear solvable over any finite-field alphabet. The network's capacity is shown to equal one, and when m is composite, its linear capacity is shown to be bounded away from one for all finite-field alphabets.

*This work was supported by the National Science Foundation.

J. Connelly and K. Zeger are with the Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, CA 92093-0407 (j2connelly@ucsd.edu and zeger@ucsd.edu).

*** Table Of Contents Provided During Manuscript Review Only ***

Contents

1	Introduction	2
1.1	Previous work	3
1.2	Our contributions	4
1.3	Preliminaries	7
2	The network $\mathcal{N}_0(m)$	9
3	The network $\mathcal{N}_1(m)$	11
3.1	Solvability conditions of $\mathcal{N}_1(m)$	11
3.2	Linear solvability conditions of $\mathcal{N}_1(m)$	12
3.3	Capacity and linear capacity of $\mathcal{N}_1(m)$	12
4	The network $\mathcal{N}_2(m, w)$	14
4.1	Solvability conditions of $\mathcal{N}_2(m, w)$	15
4.2	Linear solvability conditions of $\mathcal{N}_2(m, w)$	16
4.3	Capacity and linear capacity of $\mathcal{N}_2(m, w)$	16
5	The network $\mathcal{N}_3(m_1, m_2)$	17
5.1	Solvability conditions of $\mathcal{N}_3(m_1, m_2)$	18
5.2	Linear solvability conditions of $\mathcal{N}_3(m_1, m_2)$	19
5.3	Capacity and linear capacity of $\mathcal{N}_3(m_1, m_2)$	19
6	The network $\mathcal{N}_4(m)$	20
6.1	Solvability conditions of $\mathcal{N}_4(m)$	21
6.2	Linear solvability conditions of $\mathcal{N}_4(m)$	24
6.3	Capacity and linear capacity of $\mathcal{N}_4(m)$	25
6.4	Size of $\mathcal{N}_4(m)$	26
7	Open Questions	29
A	Appendix - Proofs of Lemmas	30
A.1	Proofs of Lemmas in Section 1	30
A.2	Proofs of Lemmas in Section 2	31
A.3	Proofs of Lemmas in Section 3	32
A.4	Proofs of Lemmas in Section 4	43
A.5	Proofs of Lemmas in Section 5	53

1 Introduction

A *network* will refer to a finite, directed, acyclic multigraph, some of whose nodes are *sources* or *receivers*. Source nodes generate k -dimensional vectors of *messages*, where each of the k messages is an arbitrary element of a fixed, finite set of size at least 2, called an *alphabet*. The elements of an alphabet are called *symbols*. The *inputs* to a node are the messages, if any, originating at the node and the symbols on the incoming edges of the node. Each outgoing edge of a network node carries a vector of n alphabet symbols, called *edge symbols*. If a node has at most n input symbols, then we will assume, without loss of generality, that each of its out-edges carries all n of such symbols. Each outgoing edge of a node has associated with it an *edge function* which maps the node's inputs to the output vector carried by the edge. Each receiver node has *demands*, which are k -dimensional message vectors the receiver wishes to obtain. Each receiver also has *decoding functions* which map the receiver's inputs to k -dimensional vectors of alphabet symbols in an attempt to satisfy the receiver's demands.

A (k, n) *fractional code over an alphabet \mathcal{A}* (or, more briefly, a (k, n) *code over \mathcal{A}*) is an assignment of edge functions to all of the edges in a network and an assignment of decoding functions to all of the receiver nodes in the network.

A (k, n) *solution over \mathcal{A}* is a (k, n) code over \mathcal{A} such that each receiver's decoding functions can recover all k components of each of its demands from its inputs.

An edge function

$$f : \underbrace{\mathcal{A}^k \times \cdots \times \mathcal{A}^k}_{i \text{ message vectors}} \times \underbrace{\mathcal{A}^n \times \cdots \times \mathcal{A}^n}_{j \text{ in-edges}} \longrightarrow \mathcal{A}^n$$

is *linear over \mathcal{A}* if it can be written in the form

$$f(x_1, \dots, x_i, y_1, \dots, y_j) = M_1 x_1 + \cdots + M_i x_i + M'_1 y_1 + \cdots + M'_j y_j \quad (1)$$

where M_1, \dots, M_i are $n \times k$ matrices and M'_1, \dots, M'_j are $n \times n$ matrices whose entries are constant values. Similarly, a decoding function is linear if it has a form analogous to (1). A (k, n) code is said to be *linear over \mathcal{A}* if each edge function and each decoding function is linear over \mathcal{A} . We will focus attention on linear codes in a very general setting where the alphabets are R -modules (discussed in in Section 1.3). If the network alphabet is an R -module, then, in (1), \mathcal{A} is an Abelian group, the elements of the matrices are from the ring R , and multiplication of ring elements by elements of \mathcal{A} is the action of the module. Special cases of linear codes over R -modules include linear codes over groups, rings, and fields.

A network is defined to be

- *solvable over \mathcal{A}* if there exists a $(1, 1)$ solution over \mathcal{A} ,
- *scalar linear solvable over \mathcal{A}* if there exists a $(1, 1)$ linear solution over \mathcal{A} ,
- *vector linear solvable over \mathcal{A}* if there exists a (k, k) linear solution over \mathcal{A} , for some $k \geq 1$,
- *asymptotically linear solvable over \mathcal{A}* if for any $\epsilon > 0$, there exists a (k, n) linear solution over \mathcal{A} for some k and n satisfying $k/n > 1 - \epsilon$.

We say that a network is *solvable*, (respectively, *vector linear solvable* or *scalar linear solvable*) if it is solvable (respectively, vector linear solvable or scalar linear solvable) over some alphabet.

The *capacity*¹ of a network is:

$$\sup\{k/n : \exists \text{ a } (k, n) \text{ solution over some } \mathcal{A}\}.$$

The *linear capacity* of a network with respect to an alphabet \mathcal{A} is:

$$\sup\{k/n : \exists \text{ a } (k, n) \text{ linear solution over } \mathcal{A}\}.$$

It was shown in [4] that the capacity of a network is independent of alphabet size, and it was noted that linear capacity can depend on alphabet size.

1.1 Previous work

One decade ago, it was demonstrated in [7] that there can exist a network which is solvable, but not vector linear solvable over any finite-field alphabet and any vector dimension. To date, the network given in [7] is the only known example of such a network published in the literature. In fact, the network given in [7] was shown to not be vector linear solvable over very general algebraic types of alphabets, such as finite rings and modules, and was shown not to even be asymptotically linear solvable over finite-field alphabets, and, as a result, the network has been described as “diabolical” by Kschischang [18]² and Koetter [16].

The diabolical network has been utilized in numerous extensions and applications of network coding, such as by Krishnan and Rajan [17] for network error correction, and by Rai and Dey [21] for multicasting the sum of messages to construct networks with equivalent solvability properties hence showing that linear codes are insufficient for each problem. El Rouayheb, Sprintson, and Georgiades [13] reduced the index coding problem to a network coding problem, thereby using the diabolical network to show that linear index codes are not necessarily sufficient. Blasiak, Kleinberg, and Lubetzky [2] used index codes to create networks where there is a polynomial separation between linear and non-linear network coding rates. Chan and Grant [5] showed a duality between entropy functions and network coding problems, which allowed for an alternative proof of the insufficiency of linear network codes.

We now summarize some of the existing results regarding the solvability and linear solvability of *multicast networks* (in which each receiver demands all of the messages) and *general networks* (in which each receiver demands a subset of the messages). Network codes were first presented by Ahlswede, Ning, Li, and Yeung [1] as a method of improving the throughput of a network; they presented the butterfly network, a variant of which is scalar linear solvable but not solvable via routing. Li, Young, and Cai [19] showed that if a multicast network is solvable, then it is scalar linear solvable over all sufficiently large finite-field alphabets. In addition, Riis [23] showed that every solvable multicast network has a binary linear solution in some vector dimension. Feder, Ron, and Tavory [14] and Rasala Lehman and Lehman [22] both independently showed that some solvable multicast networks asymptotically require finite-field alphabets to be at least as large as twice the square root of the number of receiver nodes.

¹In the literature, this is sometimes referred to as the “coding capacity” (as opposed to the routing capacity). For brevity, we will simply use the term “capacity,” as we do not discuss routing capacity in this paper.

²The terminology was apparently attributed by F. Kschischang to M. Sudan.

Non-linear coding in multicast networks can offer advantages such as reducing the alphabet size required for solvability; Rasala Lehman and Lehman [22] presented a network which is solvable over a ternary alphabet but has no scalar linear solution over any alphabet whose size is less than five, and Riis [23] and also [9] demonstrated general and multicast networks, respectively, which have scalar non-linear binary solutions but no scalar linear binary solutions. A multicast network was presented in [9] which is solvable precisely over those alphabets whose size is neither 2 nor 6, and Sun, Yin, Li, and Long [29] presented families of multicast networks which are scalar linear solvable over certain finite-field alphabets but not over all larger finite-field alphabets.

Unlike multicast networks, general networks that are solvable are not necessarily vector linear solvable, as demonstrated in [7]. Médard, Effros, Ho, and Karger [20] showed that there can exist a network which is vector linear solvable but not scalar linear solvable. Shenvi and Dey [27] showed that for networks with 2 source-receiver pairs the following are equivalent: the network is solvable, the network is vector linear solvable, the network satisfies a simple cut condition. Cai and Han [3] showed that for a particular class of networks with 3 source-receiver pairs: the solvability can be determined in polynomial time, being solvable is equivalent to being scalar linear solvable, and finite-field alphabets of size 2 or 3 are sufficient to construct scalar linear solutions. In [11], the Fano and non-Fano networks were shown to be solvable precisely over even and odd alphabets, respectively. For each integer $m \geq 2$, Rasala Lehman and Lehman [22] demonstrated a class of networks which are not solvable over any alphabet whose size is less than m and are solvable over all alphabets whose size is a prime power greater than or equal to m . For each integer $m \geq 3$, Chen and HaiBin [6] demonstrated a class of networks which are not solvable over any alphabet whose size is less than m and are solvable over all alphabets whose size is not divisible by $2, 3, \dots, m-1$.

Koetter and Médard [15] showed for every finite field \mathbb{F} and every network, the network is scalar linear solvable over \mathbb{F} if and only if a corresponding system of polynomials has a common root in \mathbb{F} , and in [8] it was shown that for every finite field \mathbb{F} and any system of polynomials there exists a corresponding network which is scalar linear solvable over \mathbb{F} if and only if the system of polynomials has a common root in \mathbb{F} . Subramanian and Thangaraj [28] showed an alternate method of deriving a system of polynomials which corresponds to the scalar linear solvability of a network, such that the degree of each polynomial equation is at most 2. Presently, there are no known algorithms for determining whether a general network is solvable.

While vector linear solvable networks are solvable networks, the converse need not be true. This paper demonstrates infinitely many such counterexamples.

There remain numerous open questions regarding the existence of solvable networks which are not vector linear solvable. Are many/most solvable networks not vector/scalar linearly solvable? Can such networks be efficiently characterized? Can such networks be algorithmically recognized? We leave these questions for future research.

1.2 Our contributions

In this paper, we present an infinite class of solvable networks which are not linear solvable over any R -module alphabet and any vector dimension. We denote each such network as \mathcal{N}_4 , and we construct \mathcal{N}_4 from several intermediate networks denoted by $\mathcal{N}_0, \mathcal{N}_1, \mathcal{N}_2$, and \mathcal{N}_3 , all of which are constructed from a fundamental network building block B . Specifically, for each positive

composite number m , we describe how to construct a network \mathcal{N}_4 which has a non-linear solution over an alphabet of size m , yet has no vector linear solution over any vector dimension and any finite field, commutative ring with identity, or R -module alphabet. In addition, such a network is not solvable over any alphabet whose size is less than m . The diabolical network in [7] was shown to be non-linear solvable over an alphabet of size 4.

We will now summarize the main results of this paper, which all appear in Section 6. The network \mathcal{N}_4 is parameterized by an arbitrary integer $m \geq 2$. Theorem 6.4 shows that \mathcal{N}_4 is solvable over an alphabet of size m . Theorem 6.5 shows, however, that \mathcal{N}_4 is never solvable over alphabets smaller than m . Theorem 6.7 shows that when m is prime, \mathcal{N}_4 has a scalar linear solution over a field of size m . In fact, for all non-prime integers m , the network \mathcal{N}_4 has no linear solution, as demonstrated by Theorems 6.8 and 6.9. In particular, Theorem 6.8 shows that when m is composite, no vector linear solution for \mathcal{N}_4 exists over any R -module, and Corollary 6.10 shows that in such case, \mathcal{N}_4 is not even asymptotically linear solvable over any finite-field alphabet. In the special case of $m = 4$, the demonstrated network \mathcal{N}_4 exhibits properties similar to the network presented in [7].

The diabolical network was shown in [7] to have capacity equal to one, whereas its linear capacity is bounded away from one for any finite-field alphabet. Analogously, we show in Theorem 6.9 that for all m , the capacity of \mathcal{N}_4 equals one, whereas for all composite m , its linear capacity over any finite-field alphabet is bounded away from one. Related capacity results are given for the constituent networks \mathcal{N}_0 (in Lemma 2.4), \mathcal{N}_1 (in Lemma 3.8), \mathcal{N}_2 (in Lemma 4.7), and \mathcal{N}_3 (in Lemma 5.8).

The rest of the paper is organized as follows. Table 1 summarizes the networks created and the results in this paper. Section 1.3 provides mathematical background and definitions. Sections 2-5 present the building block networks which are used to construct the main class of networks. Section 6 details the properties and construction of the main class of networks. For each network family, we will discuss the solvability properties, the linear solvability properties, and the capacity. The Appendix contains the proofs of every lemma in this paper. All other proofs are given in the main body of the paper.

Section 7 poses some open questions regarding solvability of networks.

Networks and Their Main Properties	Location
Network $\mathcal{N}_0(m)$	Section 2
· Consists of a block $B(m)$ together with source nodes.	Figure 2
· $4m + 6$ nodes.	Remark 2.1
· If a $(1, 1)$ code over \mathcal{A} is a solution, then the code has an Abelian group structure.	Lemma 2.2
Network $\mathcal{N}_1(m)$	Section 3
· Consists of a block $B(m)$ together with source nodes and an additional receiver.	Figure 3
· $4m + 7$ nodes.	Remark 3.1
· If solvable over \mathcal{A} , then $\gcd(\mathcal{A} , m) = 1$.	Lemma 3.2
· Scalar linear solvable over standard R -module G iff $\gcd(\text{char}(R), m) = 1$.	Lemma 3.3
· If asymptotically linear solvable over finite field \mathbb{F} , then $\text{char}(\mathbb{F}) \nmid m$.	Lemma 3.8
Network $\mathcal{N}_2(m, w)$	Section 4
· Consists of w blocks $B(m + 1)$ together with source nodes and an additional receiver.	Figure 4
· $4mw + 9w + 2$ nodes.	Remark 4.1
· If $w \geq 2$, then non-linear solvable over an alphabet of size mw .	Lemma 4.4
· If solvable over \mathcal{A} , then $\gcd(\mathcal{A} , m) \neq 1$.	Lemma 4.5
· Scalar linear solvable over standard R -module G iff $\text{char}(R) \mid m$.	Lemma 4.6
· If asymptotically linear solvable over finite field \mathbb{F} , then $\text{char}(\mathbb{F}) \mid m$.	Lemma 4.7
Network $\mathcal{N}_3(m_1, m_2)$	Section 5
· Consists of blocks $B(m_1)$ and $B(m_2)$ together with source nodes and an additional receiver.	Figure 5
· $4m_1 + 4m_2 + 12$ nodes.	Remark 5.1
· For each $s, t \geq 1$ relatively prime to m_1 , if $m_2 = sm_1^\alpha$ for some $\alpha > 0$, then non-linear solvable over an alphabet of size $tm_1^{\alpha+1}$.	Corollary 5.7
· If solvable over \mathcal{A} , then $\gcd(\mathcal{A} , m_1) = 1$ or $ \mathcal{A} \nmid m_2$.	Lemma 5.5
· Scalar linear solvable over standard R -module G iff $\gcd(\text{char}(R), m_1, m_2) = 1$.	Lemma 5.6
· If asymptotically linear solvable over finite field \mathbb{F} , then $\text{char}(\mathbb{F})$ is relatively prime to m_1 or m_2 .	Lemma 5.8
Network $\mathcal{N}_4(m)$	Section 6
· Consists of a disjoint union of various networks $\mathcal{N}_1, \mathcal{N}_2$, and \mathcal{N}_3 .	Equation (7)
· Solvable over an alphabet of size m .	Theorem 6.4
· If $ \mathcal{A} < m$, then not solvable over \mathcal{A} .	Theorem 6.5
· If m is prime, then scalar linear solvable over $\text{GF}(m)$.	Theorem 6.7
· If m is composite, then: (1) not vector linear solvable over any R -module.	Theorem 6.8
(2) not asymptotically linear solvable over any finite field.	Corollary 6.10
· Number of nodes is $O\left(m^{\frac{\log m}{\log \log m}}\right)$ and $\Omega(m)$.	Theorem 6.11

Table 1: Summary of the networks constructed in this paper, where m, m_1, m_2 , and w are integers such that $m, m_1, m_2 \geq 2$ and $w \geq 1$.

1.3 Preliminaries

The following definitions and results regarding linear network codes over R -modules are from [7] and [12].

Definition 1.1. Let $(R, +, *)$ be a ring with additive identity 0_R . An R -module (specifically a left R -module) is an Abelian group (G, \oplus) with identity 0_G and an action

$$\cdot : R \times G \rightarrow G$$

such that for all $r, s \in R$ and all $g, h \in G$ the following hold:

$$\begin{aligned} r \cdot (g \oplus h) &= (r \cdot g) \oplus (r \cdot h) \\ (r + s) \cdot g &= (r \cdot g) \oplus (s \cdot g) \\ (r * s) \cdot g &= r \cdot (s \cdot g) \\ 0_R \cdot g &= 0_G. \end{aligned}$$

The ring multiplication symbol $*$ will generally be omitted for brevity. If the ring R has a multiplicative identity 1_R , then we also require $1_R \cdot g = g$ for all $g \in G$. For brevity, we say that G is an R -module. \ominus will denote adding the inverse of an element (subtraction) within the group.

The following definition describes a class of R -modules which we will use to discuss linear solvability in this paper.

Definition 1.2. Let G be an R -module. We will say that G is a *standard R -module* if

1. R acts faithfully on G ; that is if $r, s \in R$ are such that $r \cdot g = s \cdot g$ for all $g \in G$, then $r = s$.
2. R has a multiplicative identity 1_R .
3. R is finite.
4. If $r \in R$ has a multiplicative left (respectively, right) inverse, then it has a two-sided inverse, which will be denoted r^{-1} .

This enables us to characterize over which standard R -modules the networks in this paper are scalar linear solvable. Lemmas 1.3 and 1.4 show that if a network is not scalar linear solvable over any standard R -module, then the network is not vector linear solvable over any R -module.

A finite ring R , with a multiplicative identity, acting on itself is a standard R -module. For any finite field \mathbb{F} and positive integer k , the set $M_k(\mathbb{F})$ of $k \times k$ matrices over \mathbb{F} with matrix addition and multiplication is a ring and \mathbb{F}^k is a standard $M_k(\mathbb{F})$ -module.

Lemma 1.3. *If a network \mathcal{N} is not scalar linear solvable over any standard R -module, then it is not scalar linear solvable over any R -module.*

Lemma 1.4. *If a network is not scalar linear solvable over any R -module, then it is not vector linear solvable over any R -module.*

Vector linear solutions over rings are special cases of vector linear solutions over R -modules where R acts on itself. A field is a special case of a commutative ring with identity where all elements have multiplicative inverses, and scalar linear solutions are special cases of vector linear solutions where $k = 1$. Thus if a network is not vector linear solvable over R -modules, it is also not vector (or scalar) linear solvable over rings with identity (or fields).

For any ring R with multiplicative identity, the *characteristic of R* is denoted $\text{char}(R)$ and is the smallest positive integer m such that 1_R added to itself m times equals 0_R . The characteristic of a finite field is always a prime number. We say that a positive integer m is *invertible in R* if there exists $m^{-1} \in R$ such that $m^{-1}(m1_R) = 1_R$, where $(m1_R)$ denotes 1_R added to itself m times. Specifically,

$$m^{-1} = \left(\underbrace{1_R + \cdots + 1_R}_{m \text{ adds}} \right)^{-1}.$$

The following lemmas discuss properties of multiplicative inverses in rings and will be used to more easily characterize the classes of R -modules over which \mathcal{N}_1 and \mathcal{N}_3 are scalar linear solvable.

Lemma 1.5. *For each finite ring R with a multiplicative identity and each positive integer m , the integer m is invertible in R if and only if there does not exist $s \in R \setminus \{0_R\}$ such that $ms = 0_R$.*

Lemma 1.6. *For each finite ring R with a multiplicative identity and each positive integer m , the integer m is invertible in R if and only if $\text{char}(R)$ and m are relatively prime.*

The following definition is called Property P' in [6], and will be utilized throughout.

Definition 1.7. Let $m \geq 2$. A $(1, 1)$ code for a network \mathcal{N} over an alphabet \mathcal{A} , containing messages x_0, x_1, \dots, x_m and edge symbols e_0, e_1, \dots, e_m , e , is said to have *Property $P(m)$* if there exists a binary operation $\oplus : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$ and permutations $\pi_0, \pi_1, \dots, \pi_m$ and $\sigma_0, \sigma_1, \dots, \sigma_m$ of \mathcal{A} , such that (\mathcal{A}, \oplus) is an Abelian group and the edge symbols can be written as

$$e_i = \sigma_i \left(\bigoplus_{\substack{j=0 \\ j \neq i}}^m \pi_j(x_j) \right) \quad (i = 0, 1, \dots, m)$$

$$e = \bigoplus_{j=0}^m \pi_j(x_j).$$

2 The network $\mathcal{N}_0(m)$

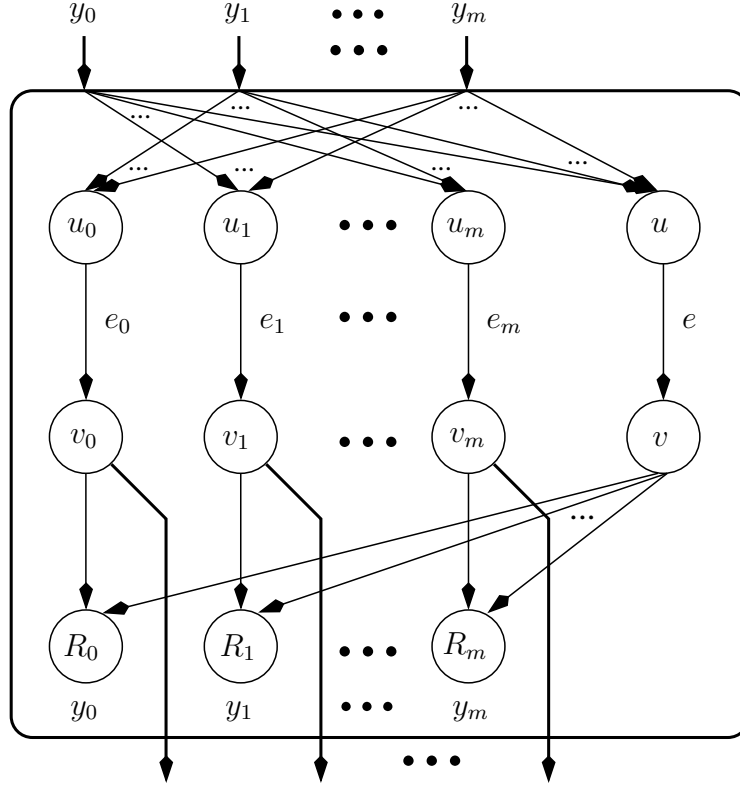


Figure 1: Network building block $B(m)$ has message inputs y_0, y_1, \dots, y_m (from unspecified source nodes) and $m + 1$ output edges. For each i , the node u_i receives each of the inputs except y_i and has a single outgoing edge to the node v_i , which carries the edge symbol e_i . The node u receives each of the inputs and has a single outgoing edge to the node v , which carries the edge symbol e . For each i , the receiver node R_i has an incoming edge from v_i and an incoming edge from v and demands the i th message y_i . The i th output edge of $B(m)$ is an outgoing edge of node v_i .

For each $m \geq 2$, the network building block $B(m)$ is defined in Figure 1 and is used to build network $\mathcal{N}_0(m)$, which is defined in Figure 2. For each i , the node v_i within $B(m)$ has a single incoming edge from node u_i , so without loss of generality, we may assume both outgoing edges of v_i carry the symbol e_i . Similarly, we may assume each of the outgoing edges of the node v carries the symbol e . Lemma 2.2 demonstrates that for each $m \geq 2$, the $(1, 1)$ solutions of network $\mathcal{N}_0(m)$ are precisely those codes which satisfy Property $P(m)$, defined in Definition 1.7. In particular, the solution alphabets have to be permutations of Abelian groups.

Remark 2.1. Network $\mathcal{N}_0(m)$ has $m + 1$ source nodes, $2(m + 2)$ intermediate nodes, and $m + 1$ receiver nodes, so the total number of nodes in $\mathcal{N}_0(m)$ is $4m + 6$.

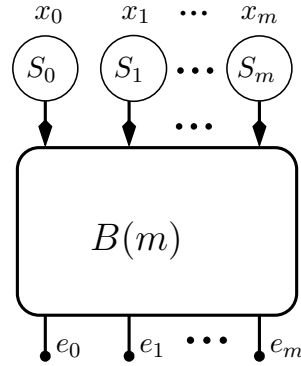


Figure 2: Network $\mathcal{N}_0(m)$ consists of a block $B(m)$ together with source nodes S_0, S_1, \dots, S_m , which generate messages x_0, x_1, \dots, x_m , respectively. The output edges of $B(m)$ are unused.

Lemma 2.2 characterizes the solvability of $\mathcal{N}_0(m)$ and will be used in the proofs of the solvability conditions of $\mathcal{N}_1, \mathcal{N}_2$, and \mathcal{N}_3 .

Lemma 2.2. *Let $m \geq 2$. A $(1, 1)$ code over an alphabet \mathcal{A} is a scalar solution for network $\mathcal{N}_0(m)$ if and only if the code satisfies Property $P(m)$.*

The following result regarding the scalar linear solvability of $\mathcal{N}_0(m)$ will be used in later proofs.

Lemma 2.3. *Let $m \geq 2$ and let G be a standard R -module. Suppose a scalar linear solution for network $\mathcal{N}_0(m)$ over G has edge symbols*

$$e_i = \bigoplus_{\substack{j=0 \\ j \neq i}}^m (c_{i,j} \cdot x_j) \quad (i = 0, 1, \dots, m)$$

$$e = \bigoplus_{j=0}^m (c_j \cdot x_j)$$

and decoding functions

$$R_i : x_i = (d_{i,e} \cdot e) \oplus (d_i \cdot e_i) \quad (i = 0, 1, \dots, m)$$

where $c_{i,j}, c_j, d_{i,e}, d_i \in R$. Then each d_i and c_i is invertible in R , and

$$c_{i,j} = -d_i^{-1} d_{i,e} c_j \quad (i, j = 0, 1, \dots, m \text{ and } j \neq i).$$

Lemma 2.4. *The network $\mathcal{N}_0(m)$ has capacity and linear capacity, for any finite-field alphabet, equal to 1.*

3 The network $\mathcal{N}_1(m)$

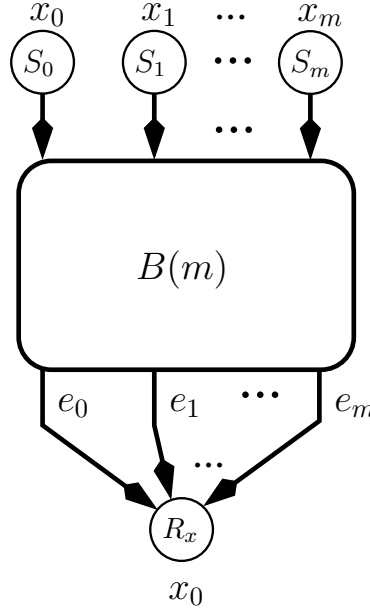


Figure 3: The network $\mathcal{N}_1(m)$ is constructed from a $B(m)$ block together with source nodes S_0, S_1, \dots, S_m and an additional receiver R_x . For each i , the source node S_i generates the message x_i and is the i th input to $B(m)$. The additional receiver R_x receives all of the output edges of $B(m)$ and demands the message x_0 .

For each $m \geq 2$, network $\mathcal{N}_1(m)$ is defined in Figure 3. The special case $m = 2$ corresponds to the non-Fano network from [10], [11], with a relabeling of messages and nodes. Lemmas 3.2, 3.3, and 3.8, respectively, demonstrate that network $\mathcal{N}_1(m)$ is

1. solvable over alphabet \mathcal{A} only if $|\mathcal{A}|$ is relatively prime to m ,
2. scalar linear solvable over standard R -module G if and only if $\text{char}(R)$ is relatively prime to m ,
3. asymptotically linear solvable over finite field \mathbb{F} if and only if $\text{char}(\mathbb{F})$ does not divide m .

Remark 3.1. Network $\mathcal{N}_1(m)$ is a network $\mathcal{N}_0(m)$ with one additional receiver node, so the total number of nodes in $\mathcal{N}_1(m)$ is $4m + 7$.

3.1 Solvability conditions of $\mathcal{N}_1(m)$

The following lemma also follows from [6, Proposition 4.1] and characterizes a condition on the alphabet size necessary for the solvability of $\mathcal{N}_1(m)$.

Lemma 3.2. For each $m \geq 2$, if network $\mathcal{N}_1(m)$ is solvable over alphabet \mathcal{A} , then m and $|\mathcal{A}|$ are relatively prime.

3.2 Linear solvability conditions of $\mathcal{N}_1(m)$

Lemma 3.3 presents a necessary and sufficient condition for the scalar linear solvability of $\mathcal{N}_1(m)$ over standard R -modules.

Lemma 3.3. *Let $m \geq 2$, and let G be a standard R -module. Then network $\mathcal{N}_1(m)$ is scalar linear solvable over G if and only if $\text{char}(R)$ is relatively prime to m .*

3.3 Capacity and linear capacity of $\mathcal{N}_1(m)$

Definition 3.4. Let \mathbb{F} be a finite field and suppose $a_1, \dots, a_q \in \mathbb{F}^{s_i}$ and $b_1, \dots, b_r \in \mathbb{F}^{t_j}$ are functions of variables x_1, \dots, x_w . We write $a_1, \dots, a_q \longrightarrow b_1, \dots, b_r$ to mean that there exist $t_j \times s_i$ matrices $M_{j,i}$ over \mathbb{F} such that for all choices of the variables x_1, \dots, x_w ,

$$b_j = \sum_{i=1}^q M_{j,i} a_i \quad (j = 1, \dots, r).$$

In the context of network coding, the variables x_1, \dots, x_w will always be taken as the network messages. In what follows, the transitive relation \longrightarrow will be used to describe linear coding functions at network nodes. Lemma 3.5 is known from linear algebra [26, p. 124], and will be used in later proofs. In particular, Lemmas 3.5, 3.6, and 3.7 will be used in bounding the linear capacities of $\mathcal{N}_1, \mathcal{N}_2$, and \mathcal{N}_3 .

Lemma 3.5. *Let \mathbb{F} be a finite field. If $A : \mathbb{F}^m \rightarrow \mathbb{F}^n$ and $B : \mathbb{F}^k \rightarrow \mathbb{F}^m$ are linear maps, then*

$$\text{rank}(A) + \text{rank}(B) - m \leq \text{rank}(AB) \quad (2)$$

$$\leq \min(\text{rank}(A), \text{rank}(B)). \quad (3)$$

Lemma 3.6. *If A is an $n \times k$ matrix of rank k over finite field \mathbb{F} , then there exists a nonsingular $n \times n$ matrix B such that*

$$BA = \begin{bmatrix} I_k \\ 0 \end{bmatrix}.$$

Lemma 3.7. *If A is an $m \times n$ matrix of rank k over finite field \mathbb{F} , then there exists an $(n - k) \times n$ matrix Q over \mathbb{F} of rank $n - k$ such that for all $x \in \mathbb{F}^n$*

$$Ax, Qx \longrightarrow x.$$

The following lemma characterizes the capacity and the linear capacity over finite-field alphabets of $\mathcal{N}_1(m)$.

Lemma 3.8. *For each $m \geq 2$, network $\mathcal{N}_1(m)$ has:*

- (a) capacity equal to 1,*
- (b) linear capacity equal to 1 for any finite-field alphabet whose characteristic does not divide m ,*
- (c) linear capacity equal to $1 - \frac{1}{2m+2}$ for any finite-field alphabet whose characteristic divides m .*

4 The network $\mathcal{N}_2(m, w)$

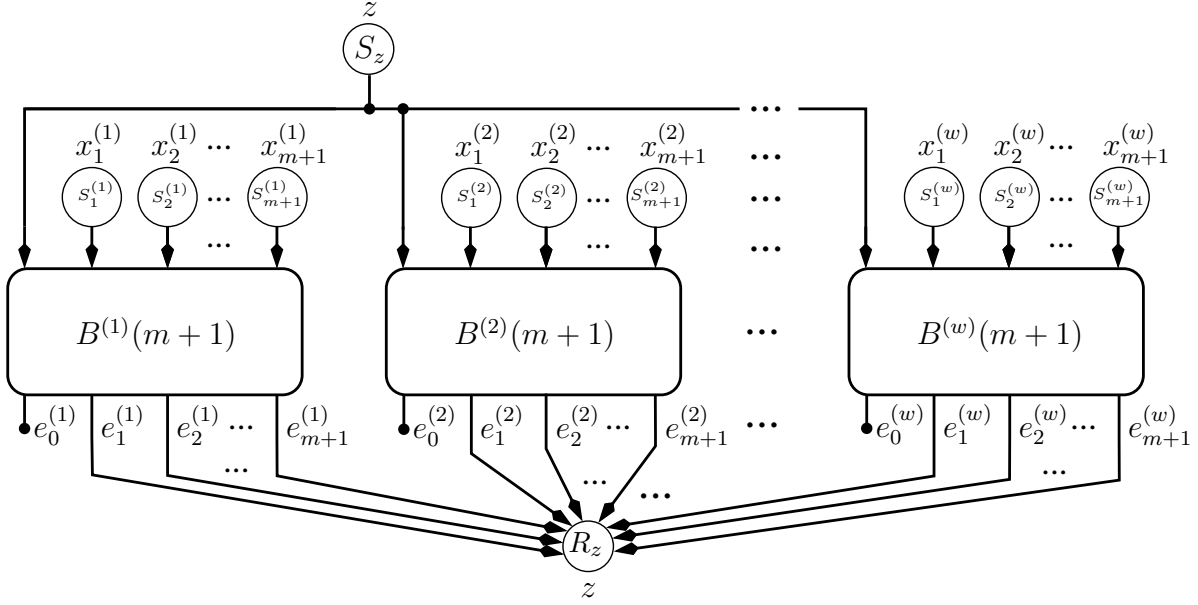


Figure 4: Network $\mathcal{N}_2(m, w)$ is constructed from w blocks of $B(m+1)$ together with $w(m+1)+1$ source nodes and an additional receiver R_z . The l th block is denoted $B^{(l)}(m+1)$, and the nodes and edge symbols within $B^{(l)}(m+1)$ are denoted with a superscript l . For each $l = 1, 2, \dots, w$, the block $B^{(l)}(m+1)$ has inputs from source nodes $S_1^{(l)}, S_2^{(l)}, \dots, S_{m+1}^{(l)}$, which generate messages $x_1^{(l)}, x_2^{(l)}, \dots, x_{m+1}^{(l)}$. The shared message z is generated by source node S_z and is the 0th input to each $B^{(l)}(m+1)$. Each of the output edges of $B^{(l)}(m+1)$, except the 0th, is an input to the shared receiver R_z , which demands the shared message z .

For each $m \geq 2$ and $w \geq 1$, network $\mathcal{N}_2(m, w)$ is defined in Figure 4. We note that $\mathcal{N}_2(m, 1)$ and $\mathcal{N}_1(m+1)$ have similar structure, but in network $\mathcal{N}_1(m+1)$ each of the output edges of $B(m+1)$ is connected to R_x , and in network $\mathcal{N}_2(m, 1)$ all but one of the output edges of $B(m+1)$ are connected to R_z . This disconnected edge causes the difference in solvability properties of the two networks. Lemmas 4.4, 4.5, 4.6, and 4.7 demonstrate that network $\mathcal{N}_2(m, w)$ is:

1. non-linear solvable over an alphabet of size mw , if $w \geq 2$,
2. solvable over alphabet \mathcal{A} only if $|\mathcal{A}|$ is not relatively prime to m ,
3. scalar linear solvable over standard R -module G if and only if $\text{char}(R)$ divides m ,
4. asymptotically linear solvable over finite field \mathbb{F} if and only if $\text{char}(\mathbb{F})$ divides m .

Remark 4.1. For each $m \geq 2$ and $w \geq 1$ network $\mathcal{N}_2(m, w)$ has $w(m+1)+1$ source nodes, $w(2m+6)$ intermediate nodes, and $w(m+2)+1$ receiver nodes, so the total number of nodes in $\mathcal{N}_2(m, w)$ is $4mw + 9w + 2$.

4.1 Solvability conditions of $\mathcal{N}_2(m, w)$

For each positive integer m , we will view the ring \mathbf{Z}_m as the set $\{0, 1, \dots, m-1\}$ together with addition and multiplication modulo m . This ring will be used to construct non-linear solutions in Lemmas 4.2, 4.4, 5.2, and 5.4.

For each $m, w \geq 2$ and $a \in \mathbf{Z}_{mw}$, a receiver cannot uniquely determine the symbol a in \mathbf{Z}_{mw} from the symbol $wa \in \mathbf{Z}_{mw}$ since w is not invertible in \mathbf{Z}_{mw} . For example, if a receiver receives $wa = 0$ in \mathbf{Z}_{mw} , then the symbol a could be any element in the set $\{0, m, 2m, \dots, (w-1)m\}$. The following lemma describes a technique for recovering the value of a via a decoding function ψ from the w -tuple $w\pi_1(a), w\pi_2(a), \dots, w\pi_w(a)$, where each π_i is a particular permutation of \mathbf{Z}_{mw} . This technique will then be used to show that network $\mathcal{N}_2(m, w)$ is solvable over an alphabet of size mw .

Lemma 4.2. *For each $m \geq 2$ and $w \geq 1$, there exist permutations $\pi_1, \pi_2, \dots, \pi_w$ of \mathbf{Z}_{mw} and a mapping $\psi : \mathbf{Z}_{mw}^w \rightarrow \mathbf{Z}_{mw}$ such that for all $a \in \mathbf{Z}_{mw}$*

$$\psi(w\pi_1(a), w\pi_2(a), \dots, w\pi_w(a)) = a.$$

Example 4.3. *The following table illustrates Lemma 4.2 for the case $m = 4$ and $w = 3$.*

$a = \pi_3(a)$	$\pi_2(a)$	$\pi_1(a)$	$3\pi_3(a)$	$3\pi_2(a)$	$3\pi_1(a)$
0	0	0	0	0	0
1	1	1	3	3	3
2	2	2	6	6	6
3	3	3	9	9	9
4	4	5	0	0	3
5	5	6	3	3	6
6	6	7	6	6	9
7	7	4	9	9	0
8	9	8	0	3	0
9	10	9	3	6	3
10	11	10	6	9	6
11	8	11	9	0	9

For each $a \in \mathbf{Z}_{12}$, the triple $(3\pi_3(a), 3\pi_2(a), 3\pi_1(a)) \in \mathbf{Z}_{12}^3$ is distinct.

Lemma 4.2 will be used in the proof of Lemma 4.4 to show that the receiver R_z can recover the message z from the set of edge symbols $e_i^{(l)}$ where $l = 1, 2, \dots, w$ and $i = 1, 2, \dots, m+1$.

Lemma 4.4. *For each $m \geq 2$ and $w \geq 1$, network $\mathcal{N}_2(m, w)$ is solvable over an alphabet of size mw .*

In the code given in the proof of Lemma 4.4, if $w = 1$, then π_1 and ψ are identity permutations, so the code is linear. However if $w > 1$, then $\pi_1, \pi_2, \dots, \pi_{w-1}$ are generally non-linear, so the code is non-linear.

Lemma 4.5. *For each $m \geq 2$ and $w \geq 1$, if network $\mathcal{N}_2(m, w)$ is solvable over alphabet \mathcal{A} , then m and $|\mathcal{A}|$ are not relatively prime.*

Lemmas 4.4 and 4.5 together provide a partial characterization of the alphabet sizes over which $\mathcal{N}_2(m, w)$ is solvable. However, these conditions are sufficient for showing our main results.

4.2 Linear solvability conditions of $\mathcal{N}_2(m, w)$

Lemma 4.6 characterizes a necessary and sufficient condition for the scalar linear solvability of $\mathcal{N}_2(m, w)$ over standard R -modules.

Lemma 4.6. *Let $m \geq 2$ and $w \geq 1$, and let G be a standard R -module. Then network $\mathcal{N}_2(m, w)$ is scalar linear solvable over G if and only if $\text{char}(R)$ divides m .*

By Lemma 4.4, for every $m, w \geq 2$, the network $\mathcal{N}_2(m, w)$ is solvable over the ring \mathbf{Z}_{mw} , but $\text{char}(\mathbf{Z}_{mw}) = mw \nmid m$ so by Lemma 4.6, the solution is necessarily non-linear.

4.3 Capacity and linear capacity of $\mathcal{N}_2(m, w)$

The following lemma provides a partial characterization of the linear capacity of $\mathcal{N}_2(m, w)$ over finite-field alphabets.

Lemma 4.7. *For each $m \geq 2$ and $w \geq 1$, network $\mathcal{N}_2(m, w)$ has*

- (a) *capacity equal to 1,*
- (b) *linear capacity equal to 1 for any finite-field alphabet whose characteristic divides m ,*
- (c) *linear capacity upper bounded by $1 - \frac{1}{2mw+2w+1}$ for any finite-field alphabet whose characteristic does not divide m .*

Improving these upper-bounds on the linear capacities and/or finding codes at these rates are left as open problems. The problems appear to be non-trivial, and such improvements are unrelated to the main results of this paper.

5 The network $\mathcal{N}_3(m_1, m_2)$

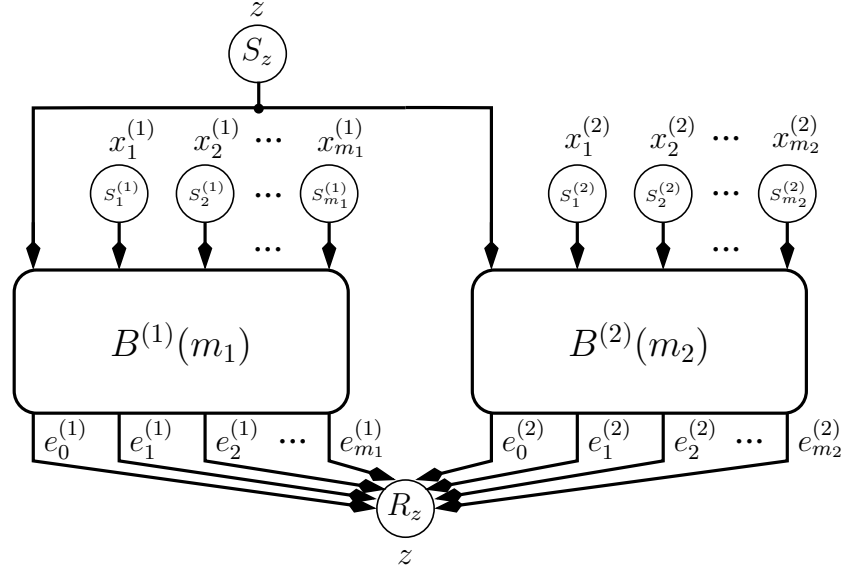


Figure 5: The network $\mathcal{N}_3(m_1, m_2)$ is constructed from $B(m_1)$ and $B(m_2)$ blocks together with $m_1 + m_2 + 1$ source nodes and an additional receiver R_z . The blocks are denoted $B^{(1)}(m_1)$ and $B^{(2)}(m_2)$ respectively, and for each $l = 1, 2$, the nodes and edge symbols in $B^{(l)}(m_l)$ are denoted with a superscript l . Each $B^{(l)}(m_l)$ block has inputs from source nodes $S_1^{(l)}, S_2^{(l)}, \dots, S_{m_l}^{(l)}$, which generate messages $x_1^{(l)}, x_2^{(l)}, \dots, x_{m_l}^{(l)}$. The shared message z is generated by source node S_z and is the 0th input to $B^{(l)}(m_l)$. The additional receiver R_z receives all of the output edges of $B^{(1)}(m_1)$ and $B^{(2)}(m_2)$ and demands the shared message z .

For each $m_1, m_2 \geq 2$, network $\mathcal{N}_3(m_1, m_2)$ is defined in Figure 5. We note that $\mathcal{N}_2(m, 2)$ and $\mathcal{N}_3(m+1, m+1)$ have similar structure, with the exception of the disconnected output edge of each $B(m+1)$ in $\mathcal{N}_2(m, 2)$. This disconnected edge causes the difference in solvability properties of the two networks. Corollary 5.7 and Lemmas 5.5, 5.6, and 5.8 demonstrate that network $\mathcal{N}_3(m_1, m_2)$ is:

1. non-linear solvable over an alphabet of size $tm_1^{\alpha+1}$, if $\alpha \geq 1$, $m_2 = sm_1^\alpha$, and s and t are relatively prime to m_1 ,
2. solvable over alphabet \mathcal{A} only if $|\mathcal{A}|$ is relatively prime to m_1 or $|\mathcal{A}|$ does not divide m_2 ,
3. scalar linear solvable over standard R -module G if and only if $\gcd(\text{char}(R), m_1, m_2) = 1$,
4. asymptotically linear solvable over finite field \mathbb{F} if and only if $\text{char}(\mathbb{F})$ is relatively prime to m_1 or m_2 .

Remark 5.1. For each $m_1, m_2 \geq 2$, the network $\mathcal{N}_3(m_1, m_2)$ has $m_1 + m_2 + 1$ source nodes, $2(m_1 + m_2 + 4)$ intermediate nodes, and $m_1 + m_2 + 3$ receiver nodes, so the total number of nodes in $\mathcal{N}_3(m_1, m_2)$ is $4m_1 + 4m_2 + 12$.

5.1 Solvability conditions of $\mathcal{N}_3(m_1, m_2)$

The following lemmas demonstrate that $\mathcal{N}_3(m_1, m_2)$ is non-linear solvable when $m_2 = sm_1^\alpha$, $\alpha \geq 1$, and s is relatively prime to m_1 . Consider the ring alphabet $\mathbf{Z}_{m_1^{\alpha+1}}$. For every $a \in \mathbf{Z}_{m_1^{\alpha+1}}$, a receiver cannot uniquely determine a symbol a in $\mathbf{Z}_{m_1^{\alpha+1}}$ from the symbols m_1a and $sm_1^\alpha a$, since m_1 is not invertible in $\mathbf{Z}_{m_1^{\alpha+1}}$. For example, if a receiver receives $m_1a = sm_1^\alpha a = 0$ in $\mathbf{Z}_{m_1^{\alpha+1}}$, then the symbol a could be any element in the set $\{0, m_1^\alpha, 2m_1^\alpha, \dots, (m_1 - 1)m_1^\alpha\}$. The following lemma describes a technique for recovering the value of a via a decoding function ψ from $m_1\pi_1(a)$ and $sm_1^\alpha\pi_2(a)$, where π_1 and π_2 are particular permutations of $\mathbf{Z}_{m_1^{\alpha+1}}$.

Lemma 5.2. *Let $m \geq 2$ and $\alpha, s \geq 1$ be integers such that s is relatively prime to m . Then there exist permutations π_1 and π_2 of $\mathbf{Z}_{m^{\alpha+1}}$ and a mapping $\psi : \mathbf{Z}_{m^{\alpha+1}}^2 \rightarrow \mathbf{Z}_{m^{\alpha+1}}$ such that for all $a \in \mathbf{Z}_{m^{\alpha+1}}$,*

$$\psi(m\pi_1(a), sm^\alpha\pi_2(a)) = a.$$

Example 5.3. *The table below illustrates Lemma 5.2 for the case $m = 2$, $s = 3$, and $\alpha = 2$, and permutations π_1 and π_2 of \mathbf{Z}_8 .*

$a = \pi_2(a)$	$\pi_1(a)$	$12\pi_2(a)$	$2\pi_1(a)$
0	0	0	0
1	4	4	0
2	1	0	2
3	5	4	2
4	2	0	4
5	6	4	4
6	3	0	6
7	7	4	6

For each $a \in \mathbf{Z}_8$, the pair $(2\pi_1(a), 12\pi_2(a)) \in \mathbf{Z}_8^2$ is distinct.

Lemma 5.2 will be used in the proof of Lemma 5.4 to show that the receiver R_z can recover the message z from the set of edge symbols $e_i^{(l)}$, where $l = 1, 2$ and $i = 0, 1, \dots, m_l$.

Lemma 5.4. *Let $m_1, m_2 \geq 2$ and $\alpha, s \geq 1$ be integers such that $m_2 = sm_1^\alpha$ and s is relatively prime to m_1 . Then network $\mathcal{N}_3(m_1, m_2)$ is solvable over an alphabet of size $m_1^{\alpha+1}$.*

In the code given in the proof of Lemma 5.4, the permutation π_1 is non-linear, so the code is non-linear.

Lemma 5.5. *Let $m_1, m_2 \geq 2$. If network $\mathcal{N}_3(m_1, m_2)$ is solvable over alphabet \mathcal{A} and $|\mathcal{A}|$ divides m_2 , then m_1 and $|\mathcal{A}|$ are relatively prime.*

Lemmas 5.4 and 5.5 together provide a partial characterization of the alphabet sizes over which $\mathcal{N}_2(m, w)$ is solvable. However, these conditions are sufficient for showing our main results.

5.2 Linear solvability conditions of $\mathcal{N}_3(m_1, m_2)$

The following lemma characterizes a necessary and sufficient condition for the scalar linear solvability of $\mathcal{N}_3(m_1, m_2)$ over standard R -modules.

Lemma 5.6. *Let $m_1, m_2 \geq 2$, and let G be a standard R -module. Then network $\mathcal{N}_3(m_1, m_2)$ is scalar linear solvable over G if and only if $\gcd(\text{char}(R), m_1, m_2) = 1$.*

Corollary 5.7. *Let $m_1, m_2 \geq 2$ and $\alpha, s, t \geq 1$ be integers such that $m_2 = sm_1^\alpha$ and s and t are relatively prime to m_1 . Then network $\mathcal{N}_3(m_1, m_2)$ is solvable over an alphabet of size $tm_1^{\alpha+1}$.*

Proof. By Lemma 5.4, network $\mathcal{N}_3(m_1, m_2)$ is solvable over an alphabet of size $m_1^{\alpha+1}$. \mathbf{Z}_t is a standard \mathbf{Z}_t -module and $\text{char}(\mathbf{Z}_t) = t$ is relatively prime to m_1 , so by Lemma 5.6, network $\mathcal{N}_3(m_1, m_2)$ is scalar linear solvable over the ring \mathbf{Z}_t .

By taking the Cartesian product code of these solutions, network $\mathcal{N}_3(m_1, m_2)$ is solvable over an alphabet of size $tm_1^{\alpha+1}$. ■

For each $m_1 \geq 2$ and $\alpha, s \geq 1$ such that s is relatively prime to m_1 , let $m_2 = m_1^\alpha s$. By Lemma 5.4, network $\mathcal{N}_3(m_1, m_2)$ is solvable over $\mathbf{Z}_{m_1^{\alpha+1}}$, but we have

$$\gcd(m_1, m_2, \text{char}(\mathbf{Z}_{m_1^{\alpha+1}})) = \gcd(m_1, m_1^\alpha s, m_1^{\alpha+1}) = m_1 \neq 1,$$

in this case, so by Lemma 5.6 the solution is necessarily non-linear. This also implies that the Cartesian product code in Corollary 5.7 is necessarily non-linear.

5.3 Capacity and linear capacity of $\mathcal{N}_3(m_1, m_2)$

Since the characteristic of any finite field is prime, the conditions of (b) and (c) of the following lemma are complements of one another.

Lemma 5.8. *For each $m_1, m_2 \geq 2$, network $\mathcal{N}_3(m_1, m_2)$ has*

- (a) *capacity equal to 1,*
- (b) *linear capacity equal to 1 for any finite-field alphabet whose characteristic is relatively prime to m_1 or m_2 ,*
- (c) *linear capacity equal to $1 - \frac{1}{2m_1 + 2m_2 + 3}$ for any finite-field alphabet whose characteristic divides m_1 and m_2 .*

6 The network $\mathcal{N}_4(m)$

A *disjoint union* of networks refers to a new network formed by combining existing networks with disjoint sets of nodes, edges, sources, and receivers. Specifically, the nodes/edges/sources/receivers in the resulting network are the disjoint union of the nodes/edges/sources/receivers in the smaller networks.

Remark 6.1. *The disjoint union of networks $\mathcal{N}_1, \dots, \mathcal{N}_w$, has a (k, n) solution over alphabet \mathcal{A} if and only if $\mathcal{N}_1, \dots, \mathcal{N}_w$ each has a (k, n) solution over \mathcal{A} .*

For any integer $m \geq 2$, let $\omega(m)$ denote the number of distinct prime factors of m . Denote the prime factorization of m by

$$m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$$

where $\gamma_1, \dots, \gamma_{\omega(m)} \geq 1$ and $p_1, \dots, p_{\omega(m)}$ are distinct primes. We define the following functions of m and its prime divisors, which will be used throughout this section:

$$f(m) = p_1^{\gamma_1-1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}-1} \quad (4)$$

$$\mu(m, i) = \min \{ \alpha \geq 0 : p_i^\alpha \geq f(m) \} \quad (i = 1, \dots, \omega(m)) \quad (5)$$

$$g(m, i) = p_i^{\gamma_i-1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega(m)} p_j^{\mu(m, j)} \quad (i = 1, \dots, \omega(m)). \quad (6)$$

For each $m \geq 2$ with prime factorization $m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$, we construct network $\mathcal{N}_4(m)$ from the following *disjoint union*³ of networks:

$$\mathcal{N}_4(m) = \left(\bigcup_{\substack{\text{prime } q \\ q \nmid m \\ q < f(m)}} \mathcal{N}_1(q) \right) \cup \left(\bigcup_{i=1}^{\omega(m)} \mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i})) \right) \cup \left(\bigcup_{\substack{i=1 \\ \gamma_i > 1}}^{\omega(m)} \mathcal{N}_3(p_i, g(m, i)) \right). \quad (7)$$

Theorem 6.2. *For each $m \geq 2$, the network $\mathcal{N}_4(m)$ is:*

1. *solvable over an alphabet of size m ,*
2. *not solvable over any alphabet whose size is less than m ,*
3. *scalar linear solvable over $\text{GF}(m)$, if m is prime,*
4. *neither vector linear solvable over any R -module alphabet nor asymptotically linear solvable over any finite-field alphabet if m is composite.*

³When node (respectively, edge and message) labels are repeated (e.g. $\mathcal{N}_1(m_1)$ and $\mathcal{N}_1(m_2)$ both have receiver R_x), add additional superscripts to each node (respectively, edge and message) to avoid repeated labels. Each disjoint network has a set of messages, nodes, and edges which is disjoint to every other network's set in the union. The messages, nodes, and edges are not directly referenced in this section, so the additional level of labeling is arbitrary so long as the networks are disjoint.

Proof. The theorem follows immediately from Theorems 6.4, 6.5, 6.7, 6.8, and Corollary 6.10. ■

Example 6.3. Consider the special cases of the square-free integer⁴ 6, the prime power 27, and the integer 100 which is neither square-free nor a prime power.

- $m = 6 = 2^1 3^1$. We have $\gamma_1 = \gamma_2 = 1$ and $f(m) = 2^{(1-1)} 3^{(1-1)} = 1$, so $\mathcal{N}_4(6)$ has neither \mathcal{N}_1 nor \mathcal{N}_3 components. Thus by (7), network $\mathcal{N}_4(6)$ is the disjoint union of networks:

$$\mathcal{N}_2(2, 3) \cup \mathcal{N}_2(3, 2).$$

- $m = 27 = 3^3$. We have $f(27) = 3^{(3-1)} = 9$, $g(27, 1) = 3^{(3-1)} = 9$, and the primes less than $f(27)$ which do not divide 27 are 2, 5, and 7. Thus by (7), network $\mathcal{N}_4(6)$ is the disjoint union of networks:

$$\mathcal{N}_1(2) \cup \mathcal{N}_1(5) \cup \mathcal{N}_1(7) \cup \mathcal{N}_2(27, 1) \cup \mathcal{N}_3(3, 9).$$

- $m = 100 = 2^2 5^2$. We have $f(100) = 2^{(2-1)} 5^{(2-1)} = 10$. Then $\mu(100, 1) = 4$, since $2^4 > f(100) > 2^3$, and $\mu(100, 2) = 2$, since $5^2 > f(100) > 5^1$. So $g(100, 1) = 2^1 5^2$, $g(100, 2) = 5^1 2^4$, and the primes less than $f(100)$ which do not divide 100 are 3 and 7. Thus by (7), network $\mathcal{N}_4(100)$ is the disjoint union of networks:

$$\mathcal{N}_1(3) \cup \mathcal{N}_1(7) \cup \mathcal{N}_2(4, 25) \cup \mathcal{N}_2(25, 4) \cup \mathcal{N}_3(2, 50) \cup \mathcal{N}_3(5, 80).$$

We will use these networks as running examples throughout this section and will refer back to these constructions.

6.1 Solvability conditions of $\mathcal{N}_4(m)$

The following lemma shows that each disjoint component of $\mathcal{N}_4(m)$ is solvable over an alphabet of size m , and therefore $\mathcal{N}_4(m)$ is solvable over an alphabet of size m . The proofs of Theorems 6.4 and 6.5 make use of the functions f , μ , and g defined in (4), (5), and (6), respectively.

Theorem 6.4. For each $m \geq 2$, network $\mathcal{N}_4(m)$ is solvable over an alphabet of size m .

Proof. Let m have prime factorization $m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$.

For each prime $q < f(m)$ such that $q \nmid m$, by (7), network $\mathcal{N}_4(m)$ contains a copy of $\mathcal{N}_1(q)$. \mathbf{Z}_m is a standard \mathbf{Z}_m -module and $\text{char}(\mathbf{Z}_m) = m$ is relatively prime to q , so by Lemma 3.3, network $\mathcal{N}_1(q)$ is scalar linear solvable over the ring \mathbf{Z}_m .

For each $i = 1, \dots, \omega(m)$, by (7), network $\mathcal{N}_4(m)$ contains a copy of $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$. By Lemma 4.4, network $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$ is solvable over an alphabet of size m .

For each $i = 1, \dots, \omega(m)$ such that $\gamma_i > 1$, by (7), network $\mathcal{N}_4(m)$ contains a copy of $\mathcal{N}_3(p_i, g(m, i))$. Also, p_i and $m/p_i^{\gamma_i}$ are relatively prime, and by (6), $g(m, i)$ is the product of

⁴An integer is *square-free* if it is not divisible by the square of any prime.

$p_i^{\gamma_i-1}$ and a term which is relatively prime to p_i , so by Corollary 5.7, network $\mathcal{N}_3(p_i, g(m, i))$ is solvable over an alphabet of size m .

Thus each disjoint component of $\mathcal{N}_4(m)$ is solvable over an alphabet of size m , so $\mathcal{N}_4(m)$ is solvable over an alphabet of size m . ■

Each network $\mathcal{N}_1, \mathcal{N}_2$, and \mathcal{N}_3 requires the alphabet size to meet some divisibility condition in order to have a solution over that alphabet. The following lemma shows that because of these conditions, there does not exist an alphabet whose size is less than m over which each component of $\mathcal{N}_4(m)$ is solvable.

Theorem 6.5. *For each $m \geq 2$, if network $\mathcal{N}_4(m)$ is solvable over alphabet \mathcal{A} , then $|\mathcal{A}| \geq m$.*

Proof. Assume to the contrary that $\mathcal{N}_4(m)$ is solvable over an alphabet \mathcal{A} such that $|\mathcal{A}| < m$. Then each disjoint component of $\mathcal{N}_4(m)$ must be solvable over \mathcal{A} .

Let m have prime factorization $m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$.

For each $i = 1, \dots, \omega(m)$, by (7), network $\mathcal{N}_4(m)$ contains a copy of $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$. Since network $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$ is solvable over \mathcal{A} , then by Lemma 4.5, p_i is not relatively prime to $|\mathcal{A}|$. Since p_i is prime, we have $p_i \mid |\mathcal{A}|$, and thus $p_1 \cdots p_{\omega(m)} \mid |\mathcal{A}|$. Let

$$\delta = \frac{|\mathcal{A}|}{p_1 \cdots p_{\omega(m)}}.$$

If $m = p_1 \cdots p_{\omega(m)}$ (i.e. m is square-free), then we contradict the assumption that $|\mathcal{A}| < m$.

So we may assume $m > p_1 \cdots p_{\omega(m)}$, which implies $\delta \geq 2$. If $\delta \geq f(m)$, then

$$|\mathcal{A}| = \delta p_1 \cdots p_{\omega(m)} \geq f(m) p_1 \cdots p_{\omega(m)} = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}} = m \quad [\text{from (4)}],$$

which again contradicts the assumption $|\mathcal{A}| < m$, so we must have $\delta < f(m)$.

In order to write the prime factorization of $|\mathcal{A}|$, let $\{q_1, \dots, q_\rho\}$ denote the set of primes which are less than $f(m)$ and do not divide m . Each prime less than $f(m)$ either divides m and is in the set $\{p_1, \dots, p_{\omega(m)}\}$ or it does not divide m and is in the set $\{q_1, \dots, q_\rho\}$. Thus δ must be a product of q_1, \dots, q_ρ and $p_1, \dots, p_{\omega(m)}$ terms, so there exist $\alpha_1, \dots, \alpha_{\omega(m)} \geq 1$ and $\beta_1, \dots, \beta_\rho \geq 0$ such that we can write $|\mathcal{A}|$ as

$$|\mathcal{A}| = p_1^{\alpha_1} \cdots p_{\omega(m)}^{\alpha_{\omega(m)}} q_1^{\beta_1} \cdots q_\rho^{\beta_\rho}. \quad (8)$$

For each prime $q < f(m)$ such that $q \nmid m$, by (7), network $\mathcal{N}_4(m)$ contains a copy of $\mathcal{N}_1(q)$. Since network $\mathcal{N}_1(q)$ is solvable over \mathcal{A} , then by Lemma 3.2, we have $\gcd(q, |\mathcal{A}|) = 1$. Thus in (8) we have $\beta_1 = \dots = \beta_\rho = 0$.

For each $i = 1, \dots, \omega(m)$ such that $\gamma_i > 1$, by (7), network $\mathcal{N}_4(m)$ contains a copy of $\mathcal{N}_3(p_i, g(m, i))$. Since network $\mathcal{N}_3(p_i, g(m, i))$ is solvable over \mathcal{A} and $p_i \mid |\mathcal{A}|$, then by Lemma 5.5,

$|\mathcal{A}|$ does not divide $g(m, i)$. Expressing $|\mathcal{A}|$ and $g(m, i)$ as their prime factorizations yields:

$$p_1^{\alpha_1} \cdots p_{\omega(m)}^{\alpha_{\omega(m)}} \nmid p_i^{\gamma_i-1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega(m)} p_j^{\mu(m,j)} \quad [\text{from (6), (8)}].$$

This implies that for each $i \in \{1, \dots, \omega(m)\}$ such that $\gamma_i > 1$, either $\alpha_i \geq \gamma_i$ or $\alpha_j \geq \mu(m, j) + 1$ for some $j \neq i$.

If there exists $j \in \{1, \dots, \omega(m)\}$ such that $\alpha_j \geq \mu(m, j) + 1$, then we have

$$\begin{aligned} |\mathcal{A}| &= p_1^{\alpha_1} \cdots p_{\omega(m)}^{\alpha_{\omega(m)}} && [\text{from (8)}] \\ &\geq p_j^{\alpha_j-1} (p_1 \cdots p_{\omega(m)}) && [\text{from } \alpha_l \geq 1] \\ &\geq p_j^{\mu(m,j)} (p_1 \cdots p_{\omega(m)}) \\ &\geq f(m) (p_1 \cdots p_{\omega(m)}) = m && [\text{from (4), (5)}], \end{aligned}$$

which contradicts the assumption that $|\mathcal{A}| < m$. So if each component of network $\mathcal{N}_4(m)$ is solvable over \mathcal{A} and $|\mathcal{A}| < m$, it must be the case that $\alpha_i \geq \gamma_i$, for each i such that $\gamma_i > 1$. If $\gamma_i = 1$, then $\alpha_i \geq 1 = \gamma_i$. So we have $\alpha_i \geq \gamma_i$ for all i , but this implies

$$\begin{aligned} |\mathcal{A}| &= p_1^{\alpha_1} \cdots p_{\omega(m)}^{\alpha_{\omega(m)}} && [\text{from (8)}] \\ &\geq p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}} = m, \end{aligned}$$

which again contradicts the assumption that $|\mathcal{A}| < m$.

Thus there does not exist an alphabet \mathcal{A} whose size is less than m such that each disjoint component of $\mathcal{N}_4(m)$ is solvable over \mathcal{A} . ■

Example 6.6. We continue our example networks $\mathcal{N}_4(6)$, $\mathcal{N}_4(27)$, and $\mathcal{N}_4(100)$.

- Suppose $\mathcal{N}_4(6)$ is solvable over an alphabet \mathcal{A} . Since $\mathcal{N}_2(2, 3)$ is solvable over \mathcal{A} , we have 2 divides $|\mathcal{A}|$. Similarly for $\mathcal{N}_2(3, 2)$, we have that 3 divides $|\mathcal{A}|$. Since 6 is the smallest positive integer that is divisible by 2 and 3, we have $|\mathcal{A}| \geq 6$.
- Suppose $\mathcal{N}_4(27)$ is solvable over an alphabet \mathcal{A} whose size is less than 27. Then
 - $\mathcal{N}_2(27, 1)$ requires $3 \mid |\mathcal{A}|$, so $|\mathcal{A}| \in \{3, 6, 9, 12, 15, 18, 21, 24\}$.
 - $\mathcal{N}_1(2)$, $\mathcal{N}_1(5)$, and $\mathcal{N}_1(7)$ require $|\mathcal{A}|$ be relatively prime to 2, 5, and 7, so $|\mathcal{A}| \notin \{6, 12, 15, 18, 21, 24\}$.
 - $\mathcal{N}_3(3, 9)$ requires $|\mathcal{A}| \nmid 9$, so $|\mathcal{A}| \notin \{3, 9\}$.

Therefore $\mathcal{N}_4(27)$ is not solvable over any alphabet whose size is less than 27.

- Suppose $\mathcal{N}_4(100)$ is solvable over an alphabet \mathcal{A} whose size is less than 100. Then
 - $\mathcal{N}_2(4, 25)$ and $\mathcal{N}_2(25, 4)$ require $10 \mid |\mathcal{A}|$, so $|\mathcal{A}| \in \{10, 20, \dots, 90\}$.

- $\mathcal{N}_1(3)$ and $\mathcal{N}_1(7)$ require $|\mathcal{A}|$ to be relatively prime to 3 and 7, so $|\mathcal{A}| \notin \{30, 60, 70, 90\}$.
- $\mathcal{N}_3(2, 50)$ requires $|\mathcal{A}| \nmid 50$, so $|\mathcal{A}| \notin \{10, 50\}$.
- $\mathcal{N}_3(5, 80)$ requires $|\mathcal{A}| \nmid 80$, so $|\mathcal{A}| \notin \{10, 20, 40, 80\}$.

Therefore $\mathcal{N}_4(100)$ is not solvable over any alphabet whose size is less than 100.

6.2 Linear solvability conditions of $\mathcal{N}_4(m)$

The following theorems show that $\mathcal{N}_4(m)$ is linear solvable if and only if m is prime.

Theorem 6.7. *For each prime p , network $\mathcal{N}_4(p)$ is scalar linear solvable over $\text{GF}(p)$.*

Proof. If p is a prime number, then $f(p) = 1$ and the power of p is one, so by (7), network $\mathcal{N}_4(p)$ consists solely of a copy of network $\mathcal{N}_2(p, 1)$. By Lemma 4.6, network $\mathcal{N}_2(p, 1)$ has a scalar linear solution over every finite-field alphabet with characteristic p . ■

Theorem 6.8. *For each composite number m , network $\mathcal{N}_4(m)$ is not vector linear solvable over any R -module.*

Proof. Let G be a standard R -module, and assume a scalar linear solution for $\mathcal{N}_4(m)$ exists over G . Since $\mathcal{N}_4(m)$ is scalar linear solvable over G , each disjoint component of $\mathcal{N}_4(m)$ is scalar linear solvable over G . Suppose m is a composite number. Then m is a product of two or more (possibly distinct) primes. We will separately consider the cases of prime powers and non-power-of-prime composite numbers.

For each prime p and integer $\gamma \geq 2$, by (7), network $\mathcal{N}_4(p^\gamma)$ contains copies of $\mathcal{N}_2(p^\gamma, 1)$ and $\mathcal{N}_3(p, p^{\gamma-1})$. Since network $\mathcal{N}_2(p^\gamma, 1)$ is scalar linear solvable over G , by Lemma 4.6, the characteristic of R divides p^γ . Since network $\mathcal{N}_3(p, p^{\gamma-1})$ is scalar linear solvable over G , by Lemma 5.6, the characteristic of R is relatively prime to p . If the characteristic of R both divides p^γ and is relatively prime to p , then the characteristic of R is 1, which only occurs in the trivial ring (of size one). Thus there is no standard R -module over which all components of network $\mathcal{N}_4(p^\gamma)$ are scalar linear solvable.

Now suppose $\omega(m) \geq 2$. Then m has prime factorization $m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$, and by (7), network $\mathcal{N}_4(m)$ contains copies of $\mathcal{N}_2(p_1^{\gamma_1}, (m/p_1^{\gamma_1}))$ and network $\mathcal{N}_2(p_2^{\gamma_2}, (m/p_2^{\gamma_2}))$. Since network $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$ is scalar linear solvable over G , by Lemma 4.6, the characteristic of R divides $p_i^{\gamma_i}$. For primes $p_1 \neq p_2$, if the characteristic of R divides both $p_1^{\gamma_1}$ and $p_2^{\gamma_2}$ then the characteristic of R is 1, which only occurs in the trivial ring. Thus there is no standard R -module over which all components of network $\mathcal{N}_4(m)$ are scalar linear solvable.

If m is a composite number, then there are no scalar linear solutions for $\mathcal{N}_4(m)$ over any standard R -module, which, by Lemmas 1.3 and 1.4 implies there are no vector linear solutions for $\mathcal{N}_4(m)$ over any R -module. ■

6.3 Capacity and linear capacity of $\mathcal{N}_4(m)$

Theorem 6.9. *For each $m \geq 2$ network $\mathcal{N}_4(m)$ has:*

- (a) *capacity equal to 1,*
- (b) *linear capacity bounded away from 1 over all finite-field alphabets, if m is composite.*

Proof. For each $m \geq 2$, by Theorem 6.4, network $\mathcal{N}_4(m)$ is solvable over an alphabet of size m , so its capacity is at least 1. Each network $\mathcal{N}_1, \mathcal{N}_2$, and \mathcal{N}_3 has capacity equal to 1, and $\mathcal{N}_4(m)$ consists of disjoint copies of $\mathcal{N}_1, \mathcal{N}_2$, and \mathcal{N}_3 , so its capacity is at most 1. Thus the capacity of $\mathcal{N}_4(m)$ is equal to 1.

For composite m , we will again separately consider the cases of prime powers and non-power-of-prime composite numbers.

For each prime p and integer $\gamma \geq 2$, by (7), network $\mathcal{N}_4(p^\gamma)$ contains copies of $\mathcal{N}_2(p^\gamma, 1)$ and $\mathcal{N}_3(p, p^{\gamma-1})$. By Lemma 4.7, network $\mathcal{N}_2(p^\gamma, 1)$ has linear capacity upper bounded by

$$1 - \frac{1}{2p^\gamma + 3}$$

for finite-field alphabets with characteristic other than p . By Lemma 5.8, network $\mathcal{N}_3(p, p^{\gamma-1})$ has linear capacity equal to

$$1 - \frac{1}{2p^{\gamma-1} + 2p + 3}$$

for finite-field alphabets with characteristic p . Whether we select a finite-field alphabet with characteristic p or characteristic other than p , the linear capacity of $\mathcal{N}_4(p^\gamma)$ is bounded away from 1, for fixed p and γ .

Now suppose $\omega(m) \geq 2$. Then m has prime factorization $m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$, and by (7), network $\mathcal{N}_4(m)$ contains copies of $\mathcal{N}_2(p_1^{\gamma_1}, (m/p_1^{\gamma_1}))$ and $\mathcal{N}_2(p_2^{\gamma_2}, (m/p_2^{\gamma_2}))$. By Lemma 4.7, network $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$ has linear capacity upper bounded by

$$1 - \frac{1}{2m + 2(m/p_i^{\gamma_i}) + 1}$$

for finite-field alphabets with characteristic other than p_i . Since $p_1 \neq p_2$, whether we select a finite-field alphabet with characteristic p_1, p_2 , or neither p_1 nor p_2 , the linear capacity is bounded away from 1, for fixed m .

Thus for any fixed composite number m , the linear capacity of network $\mathcal{N}_4(m)$ is bounded away from 1 over all finite-field alphabets. ■

Calculating the exact linear capacity of $\mathcal{N}_4(m)$ over every finite-field alphabet is left as an open problem.

Corollary 6.10. *For each composite m , network $\mathcal{N}_4(m)$ is not asymptotically linear solvable over any finite-field alphabet.*

Proof. This follows directly from the fact that for any fixed composite number m , by Theorem 6.9, the linear capacity of $\mathcal{N}_4(m)$ is bounded away from one over all finite-field alphabets. ■

6.4 Size of $\mathcal{N}_4(m)$

Depending on the prime divisors of m , the number of nodes in $\mathcal{N}_4(m)$ can be dominated by nodes from \mathcal{N}_1 networks, \mathcal{N}_2 networks, or \mathcal{N}_3 networks. The following theorem makes use of the functions $f(m)$, $\mu(m, i)$, and $g(m, i)$ defined in (4), (5), (6).

Theorem 6.11. *For each $m \geq 2$, the number of nodes in network $\mathcal{N}_4(m)$ is asymptotically*

- (a) $\Omega(m)$,
- (b) $O(m)$, when m is prime,
- (c) $O\left(\frac{m \log m}{\log \log m}\right)$, when m is square-free,
- (d) $O(m^2 / \log m)$, when m is a prime-power,
- (e) $O\left(m^{\frac{\log m}{\log \log m}}\right)$, when m is neither square-free nor a prime-power.

Proof. By Remark 3.1, the number of nodes in $\mathcal{N}_1(q)$ is $4q + 7$.

By Remark 4.1, the number of nodes in $\mathcal{N}_2(m, w)$ is $4mw + 9w + 2$.

By Remark 5.1, the number of nodes in $\mathcal{N}_3(m_1, m_2)$ is $4m_1 + 4m_2 + 12$.

By the construction of $\mathcal{N}_4(m)$ given in (7), the total number of nodes in $\mathcal{N}_4(m)$ is:

$$\left(\sum_{\substack{\text{prime } q \\ q \nmid m \\ q < f(m)}} (4q + 7) \right) + \left(\sum_{i=1}^{\omega(m)} (4m + 9(m/p_i^{\gamma_i}) + 2) \right) + \left(\sum_{\substack{i=1 \\ \gamma_i > 1}}^{\omega(m)} (4g(m, i) + 4p_i + 12) \right) \quad (9)$$

where the first, second, and third terms are the number of nodes from \mathcal{N}_1 , \mathcal{N}_2 , and \mathcal{N}_3 networks, respectively. In order to find upper and lower bounds on the total number of nodes in $\mathcal{N}_4(m)$, we will first find upper and lower bounds on the number of nodes from \mathcal{N}_1 , \mathcal{N}_2 , and \mathcal{N}_3 networks within $\mathcal{N}_4(m)$.

It is known [25, VII.27a] that

$$\sum_{\substack{\text{prime } q \\ q \leq m}} q = O\left(\frac{m^2}{\log m}\right). \quad (10)$$

If m is a square-free number, then we have $f(m) = 1$, so in this case, there are no nodes in $\mathcal{N}_4(m)$ from \mathcal{N}_1 networks. Thus for general m , we have

$$\sum_{\substack{\text{prime } q \\ q \nmid m \\ q < f(m)}} (4q + 7) \geq 0 \quad (11)$$

and

$$\sum_{\substack{\text{prime } q \\ q \nmid m \\ q < f(m)}} (4q + 7) < \sum_{\substack{\text{prime } q \\ q \leq m}} (4q + 7) = O\left(\frac{m^2}{\log m}\right) \quad [\text{from (10)}]. \quad (12)$$

The total number of nodes in $\mathcal{N}_4(m)$ from \mathcal{N}_2 networks is

$$\sum_{i=1}^{\omega(m)} (4m + 9(m/p_i^{\gamma_i}) + 2) > \sum_{i=1}^{\omega(m)} 4m = \Omega(\omega(m)m) \quad (13)$$

and

$$\sum_{i=1}^{\omega(m)} (4m + 9(m/p_i^{\gamma_i}) + 2) < \sum_{i=1}^{\omega(m)} (13m + 2) = O(\omega(m)m). \quad (14)$$

For each $i = 1, \dots, \omega(m)$ we have

$$p_i^{\mu(m,i)} < p_i f(m) \quad [\text{from (5)}] \quad (15)$$

$$g(m, i) = p_i^{\gamma_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega(m)} p_j^{\mu(m,j)} \quad [\text{from (6)}]$$

$$< p_i^{\gamma_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega(m)} p_j f(m) \quad [\text{from (15)}]$$

$$\begin{aligned} &< p_i^{\gamma_i} f(m)^{\omega(m)-1} \prod_{j=1}^{\omega(m)} p_j \\ &= p_i^{\gamma_i} f(m)^{\omega(m)-2} m \quad [\text{from (4)}]. \end{aligned} \quad (16)$$

If m is square-free, then $\gamma_i = 1$ for all i , so in this case, there are no nodes in $\mathcal{N}_4(m)$ from \mathcal{N}_3 networks. Thus for general m , we have

$$\sum_{\substack{i=1 \\ \gamma_i > 1}}^{\omega(m)} (4g(m, i) + 4p_i + 12) \geq 0. \quad (17)$$

and

$$\begin{aligned}
 \sum_{\substack{i=1 \\ \gamma_i > 1}}^{\omega(m)} (4g(m, i) + 4p_i + 12) &\leq \sum_{i=1}^{\omega(m)} 20g(m, i) && [\text{from (6)}] \\
 &< 20m f(m)^{\omega(m)-2} \sum_{i=1}^{\omega(m)} p_i^{\gamma_i} && [\text{from (16)}] \\
 &< 20m f(m)^{\omega(m)-2} \prod_{i=1}^{\omega(m)} p_i^{\gamma_i} && [\text{from } ab \geq a + b \text{ for all } a, b \geq 2] \\
 &= 20m^2 f(m)^{\omega(m)-2} \\
 &< 20m^{\omega(m)} = O(m^{\omega(m)}) && [\text{from (4)}].
 \end{aligned} \tag{18}$$

To prove part (a), consider the lower bounds of each term of (9). The total number of nodes in $\mathcal{N}_4(m)$ is lower bounded by:

$$0 + \Omega(\omega(m) m) + 0 = \Omega(\omega(m) m) = \Omega(m) \quad [\text{from (9), (11), (13), (17)}],$$

where the final equality comes from the fact $\omega(m) = \Omega(1)$, since $\omega(m) = 1$ when m is prime.

It follows from [24, Theorem 11] that

$$\omega(m) = O\left(\frac{\log m}{\log \log m}\right). \tag{19}$$

To prove parts (b)-(e), we will consider the upper bounds on the number of nodes of each term of (9). However, each term dominates in different cases, depending on the prime factors of m .

To prove parts (b) and (c), consider a square-free integer $m = p_1 \cdots p_{\omega(m)}$. Since $\gamma_i = 1$ for all i , we have $f(m) = 1$, so there are neither \mathcal{N}_1 nor \mathcal{N}_3 components in $\mathcal{N}_4(m)$. Thus there are 0 nodes from \mathcal{N}_1 and \mathcal{N}_3 components. Then by (9) and (14), the number of nodes in $\mathcal{N}_4(m)$ is $O(\omega(m) m)$. If m is prime, then $\omega(m) = 1$, so we have the desired bound. If m is not prime, then the number of nodes is $O(\omega(m) m)$, which, along with (19), yields the desired bound.

To prove part (d), consider a prime power $m = p^\gamma$, where $\gamma \geq 2$. We have $\omega(p^\gamma) = 1$, so by (14), the number of nodes from \mathcal{N}_2 components is $O(m)$, and, by (18), the number of nodes from \mathcal{N}_3 components is $O(m)$. By (12), the number of nodes from \mathcal{N}_1 components is $O(m^2 / \log m)$. Thus the number of nodes in $\mathcal{N}_4(m)$ is $O(m^2 / \log m)$.

To prove part (e), consider m which is neither a prime power (so $\omega(m) \geq 2$) nor square-free (so there are \mathcal{N}_3 components in $\mathcal{N}_4(m)$). The number of nodes in $\mathcal{N}_4(m)$ is

$$\begin{aligned}
 O\left(\frac{m^2}{\log m}\right) + O(\omega(m) m) + O(m^{\omega(m)}) &&& [\text{from (9), (12), (14), (18)}] \\
 = O(m^{\omega(m)}) &&& [\text{from } \omega(m) \geq 2],
 \end{aligned}$$

which, along with (19), yields the desired bound. ■

Example 6.12. *We continue our example networks $\mathcal{N}_4(6)$, $\mathcal{N}_4(27)$, and $\mathcal{N}_4(100)$.*

- $\mathcal{N}_4(6)$ has 97 nodes: 53 from $\mathcal{N}_2(2, 3)$ and 44 from $\mathcal{N}_2(3, 2)$.
- $\mathcal{N}_4(27)$ has 256 nodes: 15 from $\mathcal{N}_1(2)$, 27 from $\mathcal{N}_1(5)$, 35 from $\mathcal{N}_1(7)$, 119 from $\mathcal{N}_2(27, 1)$, and 60 from $\mathcal{N}_3(3, 9)$.
- $\mathcal{N}_4(100)$ has 1691 nodes: 19 from $\mathcal{N}_1(3)$, 35 from $\mathcal{N}_1(7)$, 627 from $\mathcal{N}_2(4, 25)$, 438 from $\mathcal{N}_2(25, 4)$, 220 from $\mathcal{N}_3(2, 50)$, and 352 from $\mathcal{N}_3(5, 80)$.

7 Open Questions

Below are some remaining open questions regarding linear and non-linear solvability:

1. In [7] it was shown that there exists a network which is not vector linear solvable over any R -module yet is non-linear solvable over an alphabet of size 4. We have shown that for each composite number m , there exists a network which is not vector linear solvable over any R -module yet is non-linear solvable over an alphabet of size m . Do there exist networks which are not vector linear solvable over R -modules but are non-linear solvable over some alphabet of prime size?
2. There are examples [6], [22] in the literature of solvable networks which are not solvable over any alphabet whose size is less than some m . For each $m \geq 2$, we have demonstrated a network which is solvable over an alphabet of size m but is not solvable over any alphabet whose size is less than m . For each $m \geq 2$ does there exist a network which is solvable over alphabet \mathcal{A} if and only if $|\mathcal{A}| \geq m$? Which other “interesting” sets $S \subseteq \mathbb{N}$ have the property that there exists a network which is solvable over \mathcal{A} if and only if $|\mathcal{A}| \in S$?
3. It is not currently known whether there can exist an algorithm which determines whether a network is solvable. We have demonstrated a class of solvable networks with no vector linear solutions (i.e. diabolical networks). Can there exist an algorithm which detects whether a network is diabolical?

Appendix - Proofs of Lemmas

Proofs of Lemmas in Section 1

Proof of Lemma 1.3. This follows from the proof of [7, Theorem III.4]. ■

Proof of Lemma 1.4. If R is a ring and G is an R -module, then the set $M_k(R)$ of $k \times k$ matrices over R with matrix addition and multiplication defined in the usual way, is a ring and G^k is an $M_k(R)$ -module. So any vector linear solution over an R -module is also a scalar linear solution over some other R -module. Thus if no scalar linear solutions exist, no vector linear solutions exist. ■

Proof of Lemma 1.5. Assume m is invertible in R . Then for all $s \in R$ such that $ms = 0_R$, if we multiply both sides of the equation by m^{-1} , we have $s = 0_R$.

To prove the converse, assume $ms = 0_R$ only if $s = 0_R$. Let $T = \{ms : s \in R\}$. For each $s, s' \in R$, we have $ms = ms'$ if and only if $m(s - s') = 0_R$, which implies $s = s'$, so, by assumption, $|T| = |R|$. Thus $1_R \in T$, which implies m is invertible. ■

Proof of Lemma 1.6. Assume $\text{char}(R)$ and m are not relatively prime, so they share a common factor $a > 1$. Let c and m' be integers such that $\text{char}(R) = ac$ and $m = am'$. Then we have

$$0_R = \text{char}(R) 1_R = m' \text{char}(R) 1_R = m' a c 1_R = m c 1_R = m \left(\underbrace{1_R + \cdots + 1_R}_{c \text{ adds}} \right).$$

Since $a > 1$, we have $\underbrace{1_R + \cdots + 1_R}_{c \text{ adds}} \neq 0_R$, so by Lemma 1.5, m is not invertible in R .

Conversely, assume m is not invertible in R . Then by Lemma 1.5, there exists $s \in R \setminus \{0_R\}$ such that

$$0_R = m s = \underbrace{s + \cdots + s}_{m \text{ adds}}$$

which implies the additive order of s divides m . We also have

$$\underbrace{s + \cdots + s}_{\text{char}(R) \text{ adds}} = \text{char}(R) s = 0_R,$$

which implies the additive order of s divides $\text{char}(R)$. Since $s \neq 0_R$, the additive order of s is greater than 1, and the additive order of s divides both m and $\text{char}(R)$, so they are not relatively prime. ■

Proofs of Lemmas in Section 2

Proof of Lemma 2.2. This lemma follows directly from [6, Proposition 3.2]. ■

Proof of Lemma 2.3. Equating message components at R_i yields

$$\begin{aligned} 1_R &= d_{i,e} c_i & (i = 0, 1, \dots, m) \\ 0_R &= d_{i,e} c_j + d_i c_{i,j} & (i, j = 0, 1, \dots, m \text{ and } j \neq i) \end{aligned}$$

which implies the following elements of R are invertible:

$$\begin{aligned} d_{i,e} \text{ and } c_i & & (i = 0, 1, \dots, m) \\ d_i \text{ and } c_{i,j} & & (i, j = 0, 1, \dots, m \text{ and } j \neq i). \end{aligned}$$

The result then follows by solving for $c_{i,j}$. ■

Proof of Lemma 2.4. Let G be a standard R -module. The network $\mathcal{N}_0(m)$ has the following scalar linear solution over G :

$$\begin{aligned} e_i &= \bigoplus_{\substack{j=0 \\ j \neq i}}^m x_j & (i = 0, 1, \dots, m) \\ e &= \bigoplus_{j=0}^m x_j \end{aligned}$$

and decoding at each receiver as follows:

$$R_i : e \ominus e_i = x_i \quad (i = 0, 1, \dots, m).$$

A scalar linear solution over a finite-field alphabet is a special case of a scalar linear solution over a standard R -module. Therefore $\mathcal{N}_0(m)$ is scalar linear solvable over any finite-field alphabet, so the linear capacity of $\mathcal{N}_0(m)$ for any finite-field alphabet is at least 1. The only path for message x_0 to reach the receiver R_0 is through the edge connecting nodes u and v , so its capacity is at most 1. Thus, both the capacity of $\mathcal{N}_0(m)$ and its linear capacity for any finite-field alphabet are equal to 1. ■

Proofs of Lemmas in Section 3

Proof of Lemma 3.2. Assume $\mathcal{N}_1(m)$ is solvable over \mathcal{A} . Network $\mathcal{N}_1(m)$ consists of a network $\mathcal{N}_0(m)$ with the additional receiver R_x , so by Lemma 2.2, the edge functions within $B(m)$ must satisfy Property $P(m)$. Thus, there exists an Abelian group (\mathcal{A}, \oplus) and permutations $\pi_0, \pi_1, \dots, \pi_m$ and $\sigma_0, \sigma_1, \dots, \sigma_m$ of \mathcal{A} , such that the edges carry the symbols:

$$e_i = \sigma_i \left(\bigoplus_{\substack{j=0 \\ j \neq i}}^m \pi_j(x_j) \right) \quad (i = 0, 1, \dots, m) \quad (20)$$

$$e = \bigoplus_{j=0}^m \pi_j(x_j).$$

Now suppose to the contrary that m and $|\mathcal{A}|$ share a prime factor p . By Cauchy's Theorem of Finite Groups [12, p. 93], there exists a nonzero element a in the group \mathcal{A} whose order is p . Since $p \mid m$, we have $\underbrace{a \oplus \dots \oplus a}_{m \text{ adds}} = 0$.

Define two collections of messages as follows:

$$\begin{aligned} x_j &= \pi_j^{-1}(0) & (j = 0, 1, \dots, m) \\ \hat{x}_j &= \pi_j^{-1}(a) & (j = 0, 1, \dots, m). \end{aligned}$$

Since $a \neq 0$ and each π_j is bijective, it follows that $x_j \neq \hat{x}_j$ for all j . By Property $P(m)$, we have

$$e_i = \sigma_i \left(\underbrace{0 \oplus \dots \oplus 0}_{m \text{ adds}} \right) = \sigma_i(0) \quad (i = 0, 1, \dots, m) \quad [\text{from (20)}]$$

for the messages x_0, x_1, \dots, x_m , and

$$e_i = \sigma_i \left(\underbrace{a \oplus \dots \oplus a}_{m \text{ adds}} \right) = \sigma_i(a) \quad (i = 0, 1, \dots, m) \quad [\text{from (20)}]$$

for the messages $\hat{x}_0, \hat{x}_1, \dots, \hat{x}_m$. For both collections of messages, the edge symbols e_0, e_1, \dots, e_m are the same, and therefore the decoded value x_0 at R_x must be the same. However, this contradicts the fact that $x_0 \neq \hat{x}_0$. ■

Proof of Lemma 3.3. By Lemma 1.6, m is invertible in R if and only if $\text{char}(R)$ is relatively prime to m , so it suffices to show that for each m and each standard R -module G , network $\mathcal{N}_1(m)$ is scalar linear solvable over G if and only if m is invertible in R .

Assume network $\mathcal{N}_1(m)$ is scalar linear solvable over standard R -module G . The messages are

drawn from G , and there exist $c_{i,j}, c_j \in R$, such that the edge symbols can be written as:

$$e_i = \bigoplus_{\substack{j=0 \\ j \neq i}}^m (c_{i,j} \cdot x_j) \quad (i = 0, 1, \dots, m) \quad (21)$$

$$e = \bigoplus_{j=0}^m (c_j \cdot x_j) \quad (22)$$

and there exist $d_{i,e}, d_i, d_{x,i} \in R$, such that each receiver can linearly recover its respective message from its inputs by:

$$R_i : x_i = (d_{i,e} \cdot e) \oplus (d_i \cdot e_i) \quad (i = 0, 1, \dots, m) \quad (23)$$

$$R_x : x_0 = \bigoplus_{i=0}^m (d_{x,i} \cdot e_i). \quad (24)$$

Since $\mathcal{N}_1(m)$ contains $\mathcal{N}_0(m)$, by Lemma 2.3 and (21) – (23), each c_i and each d_i is invertible in R , and

$$c_{i,j} = -d_i^{-1} d_{i,e} c_j \quad (i, j = 0, 1, \dots, m \text{ and } j \neq i). \quad (25)$$

Equating message components at R_x yields:

$$\begin{aligned} 1_R &= \sum_{i=1}^m d_{x,i} c_{i,0} && [\text{from (21), (24)}] \\ &= - \sum_{i=1}^m d_{x,i} d_i^{-1} d_{i,e} c_0 && [\text{from (25)}] \end{aligned} \quad (26)$$

and for each $j = 1, 2, \dots, m$,

$$\begin{aligned} 0_R &= \sum_{\substack{i=0 \\ i \neq j}}^m d_{x,i} c_{i,j} && [\text{from (21), (24)}] \\ &= - \left(\sum_{\substack{i=0 \\ i \neq j}}^m d_{x,i} d_i^{-1} d_{i,e} \right) c_j && [\text{from (25)}]. \end{aligned} \quad (27)$$

For each $j = 1, 2, \dots, m$, multiplying (27) on the right by $c_j^{-1} c_0$ yields

$$0_R = \sum_{\substack{i=0 \\ i \neq j}}^m d_{x,i} d_i^{-1} d_{i,e} c_0. \quad [\text{from (27)}]. \quad (28)$$

By summing (28) over $j = 1, 2, \dots, m$ and subtracting (26), we get

$$\begin{aligned} -1_R &= \sum_{j=0}^m \sum_{\substack{i=0 \\ i \neq j}}^m d_{x,i} d_i^{-1} d_{i,e} c_0 && [\text{from (26), (28)}] \\ &= m \sum_{i=0}^m d_{x,i} d_i^{-1} d_{i,e} c_0. \end{aligned}$$

Therefore, m is invertible in R .

To prove the converse, let G be a standard R -module such that m is invertible in R . Define a scalar linear code over G by:

$$\begin{aligned} e_i &= \bigoplus_{\substack{j=0 \\ j \neq i}}^m x_j && (i = 0, 1, \dots, m) \\ e &= \bigoplus_{j=0}^m x_j. \end{aligned}$$

Receiver R_i can linearly recover x_i from its received edge symbols e and e_i by:

$$R_i : e \ominus e_i = x_i \quad (i = 0, 1, \dots, m)$$

and receiver R_x can linearly recover x_0 from its received edge symbols e_0, e_1, \dots, e_m by:

$$\begin{aligned} R_x : & \left(m^{-1} \cdot \bigoplus_{i=0}^m e_i \right) \ominus e_0 \\ &= \left(m^{-1} \cdot \bigoplus_{i=0}^m \bigoplus_{\substack{j=0 \\ j \neq i}}^m x_j \right) \ominus \bigoplus_{j=1}^m x_j \\ &= \bigoplus_{j=0}^m x_j \ominus \bigoplus_{j=1}^m x_j = x_0. \end{aligned}$$

Thus the code is a scalar linear solution for $\mathcal{N}_1(m)$. ■

Proof of Lemma 3.6. It follows immediately from Gaussian elimination. ■

Proof of Lemma 3.7. Choose k independent rows of A , find $n - k$ members of \mathbb{F}^n which together with the k rows of A form a basis of \mathbb{F}^n , and let the $n - k$ members be the rows of Q . Since the rows of A together with the rows of Q form a basis of \mathbb{F}^n , there exists an $n \times m$ matrix C_1 and an $n \times (n - k)$ matrix C_2 such that for all $x \in \mathbb{F}^n$

$$x = C_1 A x + C_2 Q x.$$

The results follow immediately. ■

Proof of Lemma 3.8. Since a scalar linear solution over a finite-field alphabet is a special case of a scalar linear solution over a standard R -module, by Lemma 3.3, $\mathcal{N}_1(m)$ is scalar linear solvable over any finite-field alphabet whose characteristic does not divide m , so the network's linear capacity for such finite-field alphabets is at least 1. By Lemma 2.4, network $\mathcal{N}_0(m)$ has capacity equal to 1, and since $\mathcal{N}_1(m)$ contains $\mathcal{N}_0(m)$, the capacity of $\mathcal{N}_1(m)$ is at most 1. Thus, both the capacity of $\mathcal{N}_1(m)$ and its linear capacity for finite-field alphabets whose characteristic does not divide m are equal to 1.

To prove part (c), consider a (k, n) fractional linear solution for $\mathcal{N}_1(m)$ over a finite field \mathbb{F} whose characteristic divides m . Since $\text{char}(\mathbb{F}) \mid m$, we have $m = 0$ in \mathbb{F} .

We have $x_i \in \mathbb{F}^k$ and $e, e_i \in \mathbb{F}^n$, with $n \geq k$, since the capacity is one. There exist $n \times k$ coding matrices $M_j, M_{i,j}$ with entries in \mathbb{F} , such that the edge vectors can be written as:

$$e_i = \sum_{\substack{j=0 \\ j \neq i}}^m M_{i,j} x_j \quad (i = 0, 1, \dots, m) \quad (29)$$

$$e = \sum_{j=0}^m M_j x_j \quad (30)$$

and there exist $k \times n$ decoding matrices $D_{i,e}, D_i$ with entries in \mathbb{F} , such that each x_i can be linearly decoded at R_i from the two n -vectors e and e_i by:

$$R_i : x_i = D_{i,e} e + D_i e_i \quad (i = 0, 1, \dots, m). \quad (31)$$

Since receiver R_x linearly recovers x_0 from e_0, e_1, \dots, e_m , we can write

$$e_0, e_1, \dots, e_m \longrightarrow x_0. \quad (32)$$

For each $i = 0, 1, \dots, m$, if we set $x_i = 0$ in (31), then we get the following relationship among the remaining m messages (since e_i does not depend on x_i):

$$0 = D_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j + D_i e_i \quad (i = 0, 1, \dots, m) \quad [\text{from (29), (30), (31)}], \quad (33)$$

and thus

$$e_i \longrightarrow D_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j \quad (i = 1, 2, \dots, m) \quad [\text{from (33)}] \quad (34)$$

$$\sum_{j=1}^m M_j x_j \longrightarrow D_0 e_0 \quad [\text{from (33)}]. \quad (35)$$

For each $i = 1, \dots, m$, let $Q_{i,e}$ be the matrix Q in Lemma 3.7 corresponding to when $D_{i,e}$ is the matrix A in Lemma 3.7. Similarly, let Q_0 be the matrix Q in Lemma 3.7 corresponding to taking A to be D_0 . Let L be the following list of $2m + 1$ vector functions of x_0, x_1, \dots, x_m :

$$\begin{aligned} & Q_0 e_0, \\ & e_i, \quad (i = 1, 2, \dots, m) \\ & Q_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j \quad (i = 1, 2, \dots, m). \end{aligned}$$

We have

$$L \longrightarrow D_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j \quad (i = 1, 2, \dots, m) \quad [\text{from (34)}] \quad (36)$$

$$L \longrightarrow \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j \quad (i = 1, 2, \dots, m) \quad [\text{from Lemma 3.7, (36)}], \quad (37)$$

and

$$\begin{aligned} & \left\{ \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j : i = 1, 2, \dots, m \right\} \\ & \longrightarrow \sum_{i=1}^m \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j \\ & = m M_0 x_0 + (m - 1) \sum_{j=1}^m M_j x_j \\ & = - \sum_{j=1}^m M_j x_j \quad [\text{from char}(\mathbb{F}) \mid m]. \quad (38) \end{aligned}$$

Thus we have

$$L \longrightarrow \sum_{j=1}^m M_j x_j \quad [\text{from (37), (38)}] \quad (39)$$

$$L \longrightarrow D_0 e_0 \quad [\text{from (35), (39)}] \quad (40)$$

$$L \longrightarrow e_0 \quad [\text{from Lemma 3.7, (40)}] \quad (41)$$

$$L \longrightarrow x_0 \quad [\text{from (32), (41)}] \quad (42)$$

$$x_0, \sum_{j=1}^m M_j x_j \longrightarrow e \quad [\text{from (30)}] \quad (43)$$

$$L \longrightarrow e \quad [\text{from (39), (42), (43)}] \quad (44)$$

$$L \longrightarrow x_i \quad (i = 1, 2, \dots, m) \quad [\text{from (31), (44)}] . \quad (45)$$

We will now bound the number of independent entries in the list L . By equating message components in equation (31), we have:

$$I_k = D_{i,e} M_i \quad (i = 0, 1, \dots, m) \quad [\text{from (29), (30), (31)}] . \quad (46)$$

Since each $D_{i,e}$ and M_i are $k \times n$ and $n \times k$, respectively, and $k \leq n$, the rank of each matrix is at most k , but we also have

$$\begin{aligned} \min(\text{rank}(D_{i,e}), \text{rank}(M_i)) &\geq \text{rank}(D_{i,e} M_i) && [\text{from (3)}] \\ &= \text{rank}(I_k) = k && [\text{from (46)}] , \end{aligned}$$

and so $\text{rank}(D_{i,e}) = \text{rank}(M_i) = k$, which, by Lemma 3.7, implies

$$\text{rank}(Q_{i,e}) = n - k \quad (i = 1, 2, \dots, m). \quad (47)$$

Since $\text{rank}(M_0) = k$, by Lemma 3.6, there exists an $n \times n$ nonsingular matrix W over \mathbb{F} such that

$$WM_0 = \begin{bmatrix} I_k \\ 0_{(n-k) \times k} \end{bmatrix}. \quad (48)$$

Partition each of the $k \times n$ matrix products $D_{i,e}W^{-1}$ into a $k \times k$ block T_i to the left of a $k \times (n - k)$ block U_i :

$$D_{i,e}W^{-1} = [T_i \quad U_i] \quad (49)$$

and then let V be the following $n \times n$ matrix over \mathbb{F} :

$$V = \begin{bmatrix} I_k & U_0 \\ 0_{(n-k) \times k} & I_{n-k} \end{bmatrix}. \quad (50)$$

It is easy to verify that

$$V^{-1} = \begin{bmatrix} I_k & -U_0 \\ 0_{(n-k) \times k} & I_{n-k} \end{bmatrix}. \quad (51)$$

For each $i = 0, 1, \dots, m$, change the network encoding and decoding matrices from M_i and $D_{i,e}$, respectively, to

$$M'_i = VW M_i \quad (52)$$

$$D'_{i,e} = D_{i,e} W^{-1} V^{-1}. \quad (53)$$

We have

$$T_0 = D_{0,e} W^{-1} W M_0 = I_k \quad [\text{from (46), (48), (49)}] \quad (54)$$

and therefore

$$\begin{aligned} M'_0 &= \begin{bmatrix} I_k \\ 0 \end{bmatrix} && [\text{from (48), (50), (52)}] \\ D'_{0,e} &= [I_k \quad 0] && [\text{from (49), (51), (53), (54)}]. \end{aligned} \quad (55)$$

In this case,

$$e' = \sum_{j=0}^m M'_j x_j$$

and for each $i = 0, 1, \dots, m$, the messages can be recovered by:

$$\begin{aligned} D'_{i,e} e' + D_i e_i &= D_{i,e} W^{-1} V^{-1} \sum_{j=0}^m VW M_j x_j + D_i e_i && [\text{from (52), (53)}] \\ &= D_{i,e} e + D_i e_i = x_i && [\text{from (30), (31)}]. \end{aligned}$$

Thus, this linear code still provides a (k, n) solution.

Partition each of the matrices M_i into a $k \times k$ block R_i on top of a $(n - k) \times k$ block S_i :

$$M_i = \begin{bmatrix} R_i \\ S_i \end{bmatrix} \quad (56)$$

and let

$$\rho = \text{rank}([R_1 \quad \dots \quad R_m])$$

where $[R_1 \quad \dots \quad R_m]$ is the concatenation of the matrices R_i into a $k \times mk$ matrix. Clearly $\rho \leq k$.

We have

$$\begin{aligned} D_0 \sum_{j=1}^m M_{0,j} x_j &= D_0 e_0 = -D_{0,e} \sum_{j=1}^m M_j x_j && [\text{from (29), (33)}] \\ &= -\sum_{j=1}^m R_j x_j && [\text{from (55), (56)}]. \end{aligned}$$

This gives us

$$D_0 [M_{0,1} \ \dots \ M_{0,m}] = -[R_1 \ \dots \ R_m],$$

which implies

$$\begin{aligned} \text{rank}(D_0) &\geq \text{rank}([R_1 \ \dots \ R_m]) = \rho && [\text{from (3)}] \\ \therefore \text{rank}(Q_0) &= n - \text{rank}(D_0) \leq n - \rho. \end{aligned} \tag{57}$$

Since the matrix $[R_1 \ \dots \ R_m]$ has rank ρ , there exists a $k \times k$ permutation matrix P such that the first ρ rows of $P [R_1 \ \dots \ R_m]$ are linearly independent and the remaining $k - \rho$ rows are linear combinations of those first ρ rows. Thus, there exists a $(k - \rho) \times k$ matrix X , whose right-most $k - \rho$ columns form $I_{k-\rho}$, and such that

$$XP [R_1 \ \dots \ R_m] = 0_{(k-\rho) \times mk}. \tag{58}$$

X and P are $(k - \rho) \times k$ and $k \times k$ respectively, thus the rank of X is at most $(k - \rho)$ and the rank of P is at most k . Since the right-most columns of X form $I_{k-\rho}$, we have $\text{rank}(X) = k - \rho$, and since P is a permutation matrix, we have $\text{rank}(P) = k$. Since XP is $(k - \rho) \times k$, we have

$$\begin{aligned} k - \rho &\geq \text{rank}(XP) \\ &\geq \text{rank}(X) + \text{rank}(P) - k && [\text{from (2)}] \\ &= (k - \rho) + k - k = k - \rho \end{aligned}$$

and thus $\text{rank}(XP) = k - \rho$.

Define a $(k - \rho) \times n$ matrix Y by concatenating the product XP with an all-zero matrix as follows: $Y = [XP \ 0_{(k-\rho) \times (n-k)}]$. For each $i = 1, 2, \dots, m$ we have

$$YM_i = [XP \ 0_{(k-\rho) \times (n-k)}] \begin{bmatrix} R_i \\ S_i \end{bmatrix} = 0_{(k-\rho) \times k} \quad [\text{from (56), (58)}]. \tag{59}$$

Since, for each $i = 1, 2, \dots, m$, we have $YM_i = 0_{(k-\rho) \times k}$ and by (46), $D_{i,e}M_i = I_k$, the rows of Y and the rows of $D_{i,e}$ are linearly independent. (If v is a nontrivial linear combination of rows of $D_{i,e}$, then $vM_i \neq 0$; if v' is a nontrivial linear combination of rows of Y , then $v'M_i = 0$, so $v \neq v'$). Therefore, by Lemma 3.7, we may choose $Q_{i,e}$ such that its first $k - \rho$ rows are the rows

of Y . By (47), each vector function

$$Q_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j$$

in the list L has dimension $n - k$, but the first $k - \rho$ components of each such vector function can be written as

$$Y \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j = Y M_0 x_0 \quad [\text{from (59)}]. \quad (60)$$

If we view the message vectors x_0, x_1, \dots, x_m as random variables, each of whose k components are independent and uniformly distributed over the field \mathbb{F} , then we have the following entropy (using logarithms with base $|\mathbb{F}|$) upper bounds:

$$\begin{aligned} H(Q_0 e_0) &\leq n - \rho && [\text{from (57)}] \\ H(e_1, \dots, e_m) &\leq mn && [\text{from } e_i \in \mathbb{F}^n] \\ H\left(Q_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j : i = 1, 2, \dots, m\right) &\leq m(n - k) - (m - 1)(k - \rho) && [\text{from (47), (60)}]. \end{aligned}$$

Therefore, the entropy of all of the vector functions in the list L is bounded by summing these bounds:

$$\begin{aligned} H(L) &\leq (m(n - k) - (m - 1)(k - \rho)) + (n - \rho) + mn \\ &= (2m + 1)n - (m + 1)k - (k - \rho)(m - 2) \\ &\leq (2m + 1)n - (m + 1)k && [\text{from } \rho \leq k \text{ and } m \geq 2]. \end{aligned} \quad (61)$$

But then we have:

$$\begin{aligned} (m + 1)k &= H(x_0, x_1, \dots, x_m) && [\text{from } x_i \in \mathbb{F}^k] \\ &\leq H(L) && [\text{from (42), (45)}] \\ &\leq (2m + 1)n - (m + 1)k && [\text{from (61)}] \\ \therefore \frac{k}{n} &\leq \frac{2m + 1}{2m + 2}. \end{aligned}$$

Thus the linear capacity of $\mathcal{N}_1(m)$ for any finite-field alphabet whose characteristic divides m is upper bounded by

$$1 - \frac{1}{2m + 2}.$$

For each $y \in \mathbb{F}^m$, let $[y]_i$ denote the i th component of y . To show the upper bound on the linear capacity is tight, consider a $(2m + 1, 2m + 2)$ fractional linear code for $\mathcal{N}_1(m)$ over any finite-field

alphabet whose characteristic divides m , given by:

$$[e_0]_l = \begin{cases} \sum_{\substack{j=1 \\ j \neq l}}^m [x_j]_l & (l = 1, 2, \dots, m) \\ \sum_{j=1}^m [x_j]_l & (l = m+1, \dots, 2m+1) \\ \sum_{j=2}^m [x_j]_j & (l = 2m+2) \end{cases}$$

$$[e_i]_l = \begin{cases} \sum_{\substack{j=0 \\ j \neq i \\ j \neq l}}^m [x_j]_l & (l = 1, 2, \dots, m \text{ and } l \neq i) \\ [x_0]_{m+1} + \sum_{\substack{j=1 \\ j \neq i}}^m [x_j]_j & (l = i) \\ \sum_{\substack{j=0 \\ j \neq i}}^m [x_j]_l & (l = m+1, \dots, 2m+1) \\ [x_0]_{m+1+i} & (l = 2m+2) \end{cases} \quad (i = 1, 2, \dots, m)$$

$$[e]_l = \begin{cases} \sum_{\substack{j=0 \\ j \neq l}}^m [x_j]_l & (l = 1, 2, \dots, m) \\ \sum_{j=0}^m [x_j]_l & (l = m+1, \dots, 2m+1) \\ [x_0]_{m+1} + \sum_{j=1}^m [x_j]_j & (l = 2m+2). \end{cases}$$

For each $l = 1, 2, \dots, m$, we have

$$\sum_{\substack{i=0 \\ i \neq l}}^m [e_i]_l = \sum_{\substack{i=0 \\ i \neq l}}^m \sum_{\substack{j=0 \\ j \neq i \\ j \neq l}}^m [x_j]_l = (m-1) \sum_{\substack{j=0 \\ j \neq l}}^m [x_j]_l = - \sum_{\substack{j=0 \\ j \neq l}}^m [x_j]_l \quad [\text{from char}(\mathbb{F}) \mid m]. \quad (62)$$

For each $i = 1, 2, \dots, m$, the receivers within $B(m)$ can linearly recover all $2m+1$ components of their respective demands by:

$$R_0 : [e]_l - [e_0]_l = [x_0]_l \quad (l = 1, 2, \dots, 2m+1)$$

$$\begin{aligned} R_i : [e]_l - [e_i]_l &= [x_i]_l & (l = 1, 2, \dots, 2m+1 \text{ and } l \neq i) \\ [e]_{2m+2} - [e_i]_i &= [x_i]_i \end{aligned}$$

and the additional receiver can linearly recover all components of x_0 by:

$$\begin{aligned} R_x : -[e_0]_l - \sum_{\substack{i=0 \\ i \neq l}}^m [e_i]_l &= [x_0]_l & (l = 1, 2, \dots, m) & \quad [\text{from (62)}] \\ [e_1]_1 - [e_0]_{2m+2} &= [x_0]_{m+1} \\ [e_{l-m-1}]_{2m+2} &= [x_0]_l & (l = m+2, \dots, 2m+1). \end{aligned}$$

Thus, the code is in fact a solution for $\mathcal{N}_1(m)$. ■

Proofs of Lemmas in Section 4

Proof of Lemma 4.2. Assume $w = 1$ and let π_1 and ψ be identity permutations. For each $a \in \mathbf{Z}_{mw}$ we have

$$\psi(w\pi_1(a)) = \psi(a) = a.$$

Assume $w > 1$. By the Euclidean Division Theorem, for each integer y , there exist unique integers q_y, r_y such that $y = q_y m + r_y$ and $0 \leq r_y < m$. We have $wy = w(q_y m + r_y)$, which implies

$$wy = wr_y \pmod{mw}. \quad (63)$$

For all integers x, y we have

$$\begin{aligned} wx = wy \pmod{mw} &\iff wr_x = wr_y \pmod{mw} && [\text{from (63)}] \\ &\iff r_x = r_y && [\text{from } 0 \leq r_x, r_y < m]. \end{aligned} \quad (64)$$

For each $a = q_a m + r_a \in \mathbf{Z}_{mw}$ such that $r_a \in \{0, 1, \dots, m-1\}$, let \hat{r}_a be the unique integer in $\{0, 1, \dots, m-1\}$ such that $\hat{r}_a = r_a + 1 \pmod{m}$, and define permutations $\pi_1, \pi_2, \dots, \pi_w$ of \mathbf{Z}_{mw} as follows:

$$\pi_l(a) = \begin{cases} q_a m + \hat{r}_a & \text{if } q_a = l \\ q_a m + r_a & \text{otherwise} \end{cases} \quad (l = 1, 2, \dots, w-1) \quad (65)$$

$$\pi_w(a) = a = q_a m + r_a. \quad (66)$$

Note that for all $l = 1, 2, \dots, w-1$, the (non-linear) permutation π_l modifies the remainder r_a if $q_a = l$ and otherwise acts as the identity permutation. Also, π_w is the identity permutation. Since $a \in \mathbf{Z}_{mw}$, we have $0 \leq q_a < w$.

For each $a \in \mathbf{Z}_{mw}$ we will show the mapping $a \mapsto (w\pi_1(a), \dots, w\pi_w(a))$ is injective. For each $a, b \in \mathbf{Z}_{mw}$, suppose

$$w\pi_l(a) = w\pi_l(b) \pmod{mw} \quad (l = 1, 2, \dots, w), \quad (67)$$

where $a = q_a m + r_a$ and $b = q_b m + r_b$, with $0 \leq r_a, r_b < m$ and $0 \leq q_a, q_b < w$. Then we have

$$w\pi_w(a) = w\pi_w(b) \pmod{mw} \quad [\text{from (67)}] \quad (68)$$

$$wr_a = wr_b \pmod{mw} \quad [\text{from (63), (66), (68)}]$$

$$\therefore r_a = r_b \quad [\text{from (64)}]. \quad (69)$$

Let \hat{r}_b be the unique integer in $\{0, 1, \dots, m-1\}$ such that $\hat{r}_b = r_b + 1 \pmod{m}$. If $q_a \neq q_b$,

then without loss of generality, $q_b \neq 0$, so we have:

$$\begin{aligned} w\pi_{q_b}(a) &= w\pi_{q_b}(b) && (\text{mod } mw) && [\text{from (67)}] && (70) \\ \therefore wr_a &= w\hat{r}_b && (\text{mod } mw) && [\text{from (63), (65), (70)}] \\ \therefore r_a &= r_a + 1 && (\text{mod } m) && [\text{from (64), (69)}], \end{aligned}$$

which is a contradiction, so we must have $q_a = q_b$. Thus $a = b$.

We have shown $w\pi_l(a) = w\pi_l(b) \pmod{mw}$ for all l if and only if $a = b$. Thus a can be uniquely determined from the w -tuple $(w\pi_1(a), w\pi_2(a), \dots, w\pi_w(a))$. This implies the existence of the claimed mapping. ■

Proof of Lemma 4.4. Let $\pi_1, \pi_2, \dots, \pi_w$ and ψ be the permutations and mapping, respectively, from Lemma 4.2. Define a code for network $\mathcal{N}_2(m, w)$ over the ring \mathbf{Z}_{mw} for each $l = 1, 2, \dots, w$ by:

$$\begin{aligned} e_0^{(l)} &= \sum_{j=1}^{m+1} x_j^{(l)} \\ e_i^{(l)} &= \pi_l(z) + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} x_j^{(l)} && (i = 1, 2, \dots, m+1) \\ e^{(l)} &= \pi_l(z) + \sum_{j=1}^{m+1} x_j^{(l)}. \end{aligned}$$

For each $l = 1, 2, \dots, w$, the receivers within each $B^{(l)}(m+1)$ block can recover their respective messages as follows:

$$\begin{aligned} R_0^{(l)} &: \pi_l^{-1} \left(e^{(l)} - e_0^{(l)} \right) = z \\ R_i^{(l)} &: e^{(l)} - e_i^{(l)} = x_i^{(l)} && (i = 1, 2, \dots, m+1). \end{aligned}$$

We have

$$\begin{aligned} w \sum_{i=1}^{m+1} e_i^{(l)} &= w(m+1) \pi_l(z) + mw \sum_{j=1}^{m+1} x_j^{(l)} && (l = 1, 2, \dots, w) \\ &= w\pi_l(z) && [\text{from } mw = 0 \pmod{mw}]. \end{aligned} \quad (71)$$

Receiver R_z can recover z from its inputs as follows:

$$\begin{aligned} R_z &: \psi \left(w \sum_{i=1}^{m+1} e_i^{(1)}, w \sum_{i=1}^{m+1} e_i^{(2)}, \dots, w \sum_{i=1}^{m+1} e_i^{(w)} \right) \\ &= \psi(w\pi_1(z), w\pi_2(z), \dots, w\pi_w(z)) = z && [\text{from (71) and Lemma 4.2}]. \end{aligned}$$

Thus the network code described above is, in fact, a solution for $\mathcal{N}_2(m, w)$. ■

Proof of Lemma 4.5. Assume $\mathcal{N}_2(m, w)$ is solvable over \mathcal{A} . For each $l = 1, 2, \dots, w$, the block $B^{(l)}(m+1)$ together with source nodes $S_z, S_1^{(l)}, S_2^{(l)}, \dots, S_{m+1}^{(l)}$ forms a copy of $\mathcal{N}_0(m+1)$, so by Lemma 2.2, the edge functions within block $B^{(l)}(m+1)$ must satisfy Property $P(m+1)$. Thus, for each l , there exists an Abelian group (\mathcal{A}, \oplus_l) , with identity $0_l \in \mathcal{A}$, and permutations $\pi_0^{(l)}, \pi_1^{(l)}, \dots, \pi_{m+1}^{(l)}$ and $\sigma_0^{(l)}, \sigma_1^{(l)}, \dots, \sigma_{m+1}^{(l)}$ of \mathcal{A} , such that the edges carry the symbols:

$$\begin{aligned} e_0^{(l)} &= \sigma_0^{(l)} \left(\bigoplus_{j=1}^{m+1} \pi_j^{(l)} \left(x_j^{(l)} \right) \right) \\ e_i^{(l)} &= \sigma_i^{(l)} \left(\pi_0^{(l)}(z) \oplus_l \bigoplus_{\substack{j=1 \\ j \neq i}}^{m+1} \pi_j^{(l)} \left(x_j^{(l)} \right) \right) \quad (i = 1, 2, \dots, m+1) \\ e^{(l)} &= \pi_0^{(l)}(z) \oplus_i \bigoplus_{j=1}^{m+1} \pi_j^{(l)} \left(x_j^{(l)} \right), \end{aligned} \tag{72}$$

where \bigoplus in each of the previous three equations denotes \oplus_l .

Now suppose to the contrary that m and $|\mathcal{A}|$ are relatively prime. Then by Cauchy's Theorem, for each group (\mathcal{A}, \oplus_l) there are no non-identity elements whose order divides m . That is, for each \oplus_l and each $a \in \mathcal{A}$, we have $\underbrace{a \oplus_l \dots \oplus_l a}_{m \text{ adds}} = 0_l$ if and only if $a = 0_l$. So for each $l = 1, 2, \dots, w$

let $a, b \in \mathcal{A}$. We have

$$\begin{aligned} \underbrace{a \oplus_l \dots \oplus_l a}_{m \text{ adds}} &= \underbrace{b \oplus_l \dots \oplus_l b}_{m \text{ adds}} \iff \underbrace{(a \ominus_l b) \oplus_l \dots \oplus_l (a \ominus_l b)}_{m \text{ adds}} = 0_l \quad [\text{from } (\mathcal{A}, \oplus_l) \text{ Abelian}] \\ &\iff a = b \quad [\text{from } \gcd(m, |\mathcal{A}|) = 1]. \end{aligned}$$

Thus, for each l the mapping $a \mapsto \underbrace{a \oplus_l \dots \oplus_l a}_{m \text{ adds}}$ is injective on the finite set \mathcal{A} and therefore is bijective, and its inverse $\phi_l : \mathcal{A} \rightarrow \mathcal{A}$ satisfies

$$\underbrace{\phi_l(a) \oplus_l \dots \oplus_l \phi_l(a)}_{m \text{ adds}} = a \quad (l = 1, 2, \dots, w). \tag{73}$$

For each $a \in \mathcal{A}$ such that $a \neq 0_1$, let

$$f_l(a) = \pi_0^{(l)} \left(\pi_0^{(1)^{-1}}(0_1) \right) \ominus_l \pi_0^{(l)} \left(\pi_0^{(1)^{-1}}(a) \right) \quad (l = 2, \dots, w), \tag{74}$$

and define two collections of messages as follows:

$$\begin{aligned}
 x_j^{(1)} &= \pi_j^{(1)^{-1}}(\phi_1(a)) & (j = 1, 2, \dots, m+1) \\
 z &= \pi_0^{(1)^{-1}}(0_1) \\
 x_j^{(l)} &= \pi_j^{(l)^{-1}}(0_l) & (l = 2, \dots, w) \\
 & & (j = 1, 2, \dots, m+1) \\
 \hat{x}_j^{(1)} &= \pi_j^{(1)^{-1}}(0_1) & (j = 1, 2, \dots, m+1) \\
 \hat{z} &= \pi_0^{(1)^{-1}}(a) \\
 \hat{x}_j^{(l)} &= \pi_j^{(l)^{-1}}(\phi_l(f_l(a))) & (l = 2, \dots, w) \\
 & & (j = 1, 2, \dots, m+1).
 \end{aligned}$$

Since $a \neq 0_1$ and $\pi_0^{(1)}$ is bijective, it follows that $z \neq \hat{z}$. By Property $P(m+1)$ and (72), for each $i = 1, 2, \dots, m+1$ we have:

$$\begin{aligned}
 e_i^{(1)} &= \sigma_i^{(1)} \left(\underbrace{\phi_1(a) \oplus_1 \dots \oplus_1 \phi_1(a)}_{m \text{ adds}} \right) = \sigma_i^{(1)}(a) & [\text{from (73)}] \\
 e_i^{(l)} &= \sigma_i^{(l)} \left(\pi_0^{(l)} \left(\pi_0^{(1)^{-1}}(0_1) \right) \right) & (l = 2, \dots, w)
 \end{aligned}$$

for the messages $x_j^{(l)}$, z , and

$$\begin{aligned}
 e_i^{(1)} &= \sigma_i^{(1)}(a) \\
 e_i^{(l)} &= \sigma_i^{(l)} \left(\pi_0^{(l)} \left(\pi_0^{(1)^{-1}}(a) \right) \oplus_l \underbrace{\phi_l(f_l(a)) \oplus_l \dots \oplus_l \phi_l(f_l(a))}_{m \text{ adds}} \right) & (l = 2, \dots, w) \\
 &= \sigma_i^{(l)} \left(\pi_0^{(l)} \left(\pi_0^{(1)^{-1}}(a) \right) \oplus_l f_l(a) \right) & [\text{from (73)}] \\
 &= \sigma_i^{(l)} \left(\pi_0^{(l)} \left(\pi_0^{(1)^{-1}}(0_1) \right) \right) & [\text{from (74)}].
 \end{aligned}$$

for the messages $\hat{x}_j^{(l)}$, \hat{z} . For both collections of messages, the edge symbols $e_i^{(l)}$ are the same for all $l = 1, 2, \dots, w$ and $i = 1, 2, \dots, m+1$, and therefore the decoded value z at R_z must be the same. However, this contradicts the fact that $z \neq \hat{z}$. ■

Proof of Lemma 4.6. For any ring R with multiplicative identity 1_R , the characteristic of R divides m if and only if $m = m1_R = 0_R$, so it suffices to show that for each m, w and each standard R -module G , network $\mathcal{N}_2(m, w)$ is scalar linear solvable over G if and only if $m = 0_R$.

Assume network $\mathcal{N}_2(m, w)$ is scalar linear solvable over standard R -module G . The messages are drawn from G , and there exist $c_{i,j}^{(l)}, c_j^{(l)} \in R$, such that for each $l = 1, 2, \dots, w$, the edge symbols

can be written as:

$$e_0^{(l)} = \bigoplus_{j=1}^{m+1} \left(c_{0,j}^{(l)} \cdot x_j^{(l)} \right) \quad (75)$$

$$e_i^{(l)} = \left(c_{i,0}^{(l)} \cdot z \right) \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m+1} \left(c_{i,j}^{(l)} \cdot x_j^{(l)} \right) \quad (i = 1, 2, \dots, m+1) \quad (76)$$

$$e^{(l)} = \left(c_0^{(l)} \cdot z \right) \oplus \bigoplus_{j=1}^{m+1} \left(c_j^{(l)} \cdot x_j^{(l)} \right) \quad (77)$$

and there exist $d_{i,e}^{(l)}, d_i^{(l)}, d_{z,i}^{(l)} \in R$, such that each receiver can linearly recover its respective message from its received edge symbols by:

$$R_0^{(l)} : z = \left(d_{0,e}^{(l)} \cdot e^{(l)} \right) \oplus \left(d_0^{(l)} \cdot e_0^{(l)} \right) \quad (l = 1, 2, \dots, w) \quad (78)$$

$$R_i^{(l)} : x_i^{(l)} = \left(d_{i,e}^{(l)} \cdot e^{(l)} \right) \oplus \left(d_i^{(l)} \cdot e_i^{(l)} \right) \quad \begin{matrix} (l = 1, 2, \dots, w) \\ (i = 1, 2, \dots, m+1) \end{matrix} \quad (79)$$

$$R_z : z = \bigoplus_{l=1}^w \bigoplus_{i=1}^{m+1} \left(d_{z,i}^{(l)} \cdot e_i^{(l)} \right). \quad (80)$$

For each $l = 1, 2, \dots, w$, the block $B^{(l)}(m+1)$ together with source nodes $S_z, S_1^{(l)}, S_2^{(l)}, \dots, S_{m+1}^{(l)}$ forms a copy of $\mathcal{N}_0(m+1)$, so by Lemma 2.3 and (75) – (79), each $c_i^{(l)}$ and each $d_i^{(l)}$ is invertible in R , and

$$c_{i,j}^{(l)} = - \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_j^{(l)} \quad \begin{matrix} (l = 1, 2, \dots, w) \\ (i, j = 0, 1, \dots, m+1 \text{ and } j \neq i). \end{matrix} \quad (81)$$

Equating message components at R_z yields:

$$\begin{aligned} 1_R &= \sum_{l=1}^w \sum_{i=1}^{m+1} d_{z,i}^{(l)} c_{i,0}^{(l)} && [\text{from (76), (80)}] \\ &= - \sum_{l=1}^w \sum_{i=1}^{m+1} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_0^{(l)} && [\text{from (81)}] \end{aligned} \quad (82)$$

and for each $l = 1, 2, \dots, w$,

$$\begin{aligned} 0_R &= \sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)} c_{i,j}^{(l)} & (j = 1, 2, \dots, m+1) & \quad [\text{from (76), (80)}] \\ &= - \left(\sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} \right) c_j^{(l)} & (j = 1, 2, \dots, m+1) & \quad [\text{from (81)}]. \end{aligned} \quad (83)$$

For each $l = 1, 2, \dots, w$, by multiplying (83) by $\left(c_j^{(l)} \right)^{-1} c_0^{(l)}$, we have

$$0_R = \sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_0^{(l)} \quad (j = 1, 2, \dots, m+1) \quad [\text{from (83)}]$$

and by summing over $j = 1, 2, \dots, m+1$ we have

$$\begin{aligned} 0_R &= \sum_{j=1}^{m+1} \sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_0^{(l)} \\ &= m \sum_{i=1}^{m+1} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_0^{(l)}. \end{aligned} \quad (84)$$

By summing (84) over $l = 1, 2, \dots, w$, we have

$$\begin{aligned} 0_R &= m \sum_{i=1}^w \sum_{i=1}^{m+1} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_0^{(l)} & [\text{from (84)}] \\ \therefore 0_R &= m & [\text{from (82)}]. \end{aligned}$$

To prove the converse, let G be a standard R -module such that $m 1_R = 0_R$. Define a scalar linear code over G , for each $l = 1, 2, \dots, w$, by:

$$\begin{aligned} e_0^{(l)} &= \bigoplus_{j=1}^{m+1} x_j^{(l)} \\ e_i^{(l)} &= z \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m+1} x_j^{(l)} & (i = 1, 2, \dots, m+1) \\ e^{(l)} &= z \oplus \bigoplus_{j=1}^{m+1} x_j^{(l)}. \end{aligned}$$

For each $l = 1, 2, \dots, w$, the receivers within each $B^{(l)}(m+1)$ block can linearly recover their respective messages as follows:

$$\begin{aligned} R_0^{(l)} : e^{(l)} \ominus e_0^{(l)} &= z \\ R_i^{(l)} : e^{(l)} \ominus e_i^{(l)} &= x_i^{(l)} \quad (i = 1, 2, \dots, m+1). \end{aligned}$$

Receiver R_z can linearly recover z as follows:

$$R_z : \bigoplus_{i=1}^{m+1} e_i^{(1)} = z \oplus (mz) \oplus \left(m \bigoplus_{j=1}^{m+1} x_j^{(1)} \right) = z \quad [\text{from } m = 0_R].$$

Thus the code is a scalar linear solution for $\mathcal{N}_2(m, w)$. ■

Proof of Lemma 4.7. Since a scalar linear solution over a finite-field alphabet is a special case of a scalar linear solution over a standard R -module, by Lemma 4.6, $\mathcal{N}_2(m, w)$ is scalar linear solvable over any finite-field alphabet whose characteristic divides m , so the linear capacity for such finite-field alphabets is at least 1. By Lemma 2.4, network $\mathcal{N}_0(m+1)$ has capacity equal to 1, and the block $B^{(1)}(m+1)$ together with the source nodes $S_z, S_1^{(1)}, S_2^{(1)}, \dots, S_{m+1}^{(1)}$ forms a copy of $\mathcal{N}_0(m+1)$, so the capacity of $\mathcal{N}_2(m, w)$ is at most 1. Thus both the capacity of $\mathcal{N}_2(m, w)$ and its linear capacity over any finite-field alphabet whose characteristic divides m are 1.

To prove part (c), consider a (k, n) fractional linear solution for $\mathcal{N}_2(m, w)$ over a finite field \mathbb{F} whose characteristic does not divide m . Since $\text{char}(\mathbb{F}) \nmid m$, the integer m is invertible in \mathbb{F} .

We have $x_j^{(l)}, z \in \mathbb{F}^k$ and $e_i^{(l)}, e^{(l)} \in \mathbb{F}^n$, with $n \geq k$, since the capacity is one. There exist $n \times k$ coding matrices $M_j^{(l)}, M_{i,j}^{(l)}$ over \mathbb{F} , such that for each $l = 1, 2, \dots, w$ the edge vectors can be written as:

$$\begin{aligned} e_0^{(l)} &= \sum_{j=1}^{m+1} M_{0,j}^{(l)} x_j^{(l)} \\ e_i^{(l)} &= M_{i,0}^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_{i,j}^{(l)} x_j^{(l)} \quad (i = 1, 2, \dots, m+1) \end{aligned} \tag{85}$$

$$e^{(l)} = M_0^{(l)} z + \sum_{j=1}^{m+1} M_j^{(l)} x_j^{(l)} \tag{86}$$

and there exist $k \times n$ decoding matrices $D_{i,e}^{(l)}$ and $D_i^{(l)}$ over \mathbb{F} , such that for each $l = 1, 2, \dots, w$ the message $x_i^{(l)}$ can be linearly decoded at $R_i^{(l)}$ from the n -vectors $e_i^{(l)}$ and $e^{(l)}$ by:

$$R_i^{(l)} : x_i^{(l)} = D_{i,e}^{(l)} e^{(l)} + D_i^{(l)} e_i^{(l)} \quad (i = 1, 2, \dots, m+1). \tag{87}$$

Since receiver R_z linearly recovers z from its incoming edge vectors, we have

$$\left\{ e_i^{(l)} : \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right\} \longrightarrow z. \quad (88)$$

For each $l = 1, 2, \dots, w$ and $i = 1, 2, \dots, m+1$, if we set $x_i^{(l)} = 0$ in (87), then, since $e_i^{(l)}$ does not depend on $x_i^{(l)}$, we get the following relationship among the remaining messages:

$$0 = D_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) + D_i^{(l)} e_i^{(l)} \quad [\text{from (85), (86), (87)}] \quad (89)$$

and thus

$$e_i^{(l)} \longrightarrow D_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) \quad \begin{array}{l} (l = 1, 2, \dots, w) \\ (i = 1, 2, \dots, m+1) \end{array} \quad [\text{from (89)}]. \quad (90)$$

For each $l = 1, 2, \dots, w$ and $i = 1, 2, \dots, m+1$, let $Q_{i,e}^{(l)}$ be the matrix Q in Lemma 3.7 corresponding to when $D_{i,e}^{(l)}$ is the matrix A in Lemma 3.7.

For each $l = 1, 2, \dots, w$, let $L^{(l)}$ be the following list of $2(m+1)$ vector functions of $z, x_1^{(l)}, x_2^{(l)}, \dots, x_{m+1}^{(l)}$:

$$\begin{aligned} Q_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) & \quad (i = 1, 2, \dots, m+1) \\ e_i^{(l)} & \quad (i = 1, 2, \dots, m+1). \end{aligned}$$

For each $l = 1, 2, \dots, w$ we have

$$L^{(l)} \longrightarrow D_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq l}}^{m+1} M_j^{(l)} x_j^{(l)} \right) \quad (i = 1, 2, \dots, m+1) \quad [\text{from (90)}] \quad (91)$$

$$L^{(l)} \longrightarrow M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \quad (i = 1, 2, \dots, m+1) \quad [\text{from Lemma 3.7, (91)}], \quad (92)$$

and

$$\begin{aligned}
 & z, \left\{ M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} : i = 1, 2, \dots, m+1 \right\} \\
 & \longrightarrow \sum_{i=1}^{m+1} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) - M_0^{(l)} z \\
 & = (m+1) M_0^{(l)} z + m \sum_{j=1}^{m+1} M_j^{(l)} x_j^{(l)} - M_0^{(l)} z \\
 & = m e^{(l)} \longrightarrow e^{(l)} \quad [\text{from (86) and } \text{char}(\mathbb{F}) \nmid m]. \quad (93)
 \end{aligned}$$

We also have

$$L^{(1)}, \dots, L^{(w)} \longrightarrow z \quad [\text{from (88)}] \quad (94)$$

and for each $l = 1, 2, \dots, w$

$$L^{(l)}, z \longrightarrow e^{(l)} \quad [\text{from (92), (93)}] \quad (95)$$

$$L^{(l)}, z \longrightarrow x_i^{(l)} \quad (i = 1, 2, \dots, m+1) \quad [\text{from (87), (95)}]. \quad (96)$$

Thus

$$L^{(1)}, \dots, L^{(w)} \longrightarrow z, \left\{ x_i^{(l)} : \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right\} \quad [\text{from (94), (96)}]. \quad (97)$$

We will now bound the number of independent entries in each list $L^{(l)}$.

By equating message components in equation (87), we have:

$$I_k = D_{i,e}^{(l)} M_i^{(l)} \quad \begin{array}{l} (l = 1, 2, \dots, w) \\ (i = 1, 2, \dots, m+1) \end{array} \quad [\text{from (85), (86), (87)}] \quad (98)$$

Since each $D_{i,e}^{(l)}$ is $k \times n$ and $k \leq n$, the rank of each matrix is at most k , but we also have

$$\text{rank} \left(D_{i,e}^{(l)} \right) \geq \text{rank} \left(D_{i,e}^{(l)} M_i^{(l)} \right) = \text{rank} (I_k) = k \quad [\text{from (3), (98)}],$$

and so $\text{rank} \left(D_{i,e}^{(l)} \right) = k$. By Lemma (3.7), this implies $\text{rank} \left(Q_{i,e}^{(l)} \right) = n - k$. Therefore each

vector function

$$Q_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) \quad \begin{array}{l} (l = 1, 2, \dots, w) \\ (i = 1, 2, \dots, m+1) \end{array}$$

in the list $L^{(l)}$ has dimension $n - k$.

If we view the messages vectors as random variables, each of whose k components are independent and uniformly distributed over the field \mathbb{F} , then we have the following entropy (using logarithms base $|\mathbb{F}|$) upper bounds:

$$H \left(Q_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) : \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right) \leq w(m+1)(n-k) \quad (99)$$

$$H \left(e_i^{(l)} : \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right) \leq w(m+1)n. \quad (100)$$

Therefore, the entropy of all of the vector functions in the list of lists $L^{(1)}, \dots, L^{(w)}$ is bounded by summing the bounds in (99) and (100):

$$H(L^{(1)}, \dots, L^{(w)}) \leq w(m+1)n - w(m+1)k \quad [\text{from (99), (100)}]. \quad (101)$$

But then we have:

$$\begin{aligned} (w(m+1) + 1)k &= H \left(z, \left\{ x_i^{(l)} : \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right\} \right) && [\text{from } z, x_i^{(l)} \in \mathbb{F}^k] \\ &\leq H(L^{(1)}, \dots, L^{(w)}) && [\text{from (97)}] \\ &\leq 2w(m+1)n - w(m+1)k && [\text{from (101)}] \\ \therefore \frac{k}{n} &\leq \frac{2w(m+1)}{2w(m+1) + 1}. \end{aligned}$$

Thus the linear capacity of $\mathcal{N}_2(m, w)$ for finite-field alphabets whose characteristic does not divide m is upper bounded by

$$1 - \frac{1}{2mw + 2w + 1}.$$

■

Proofs of Lemmas in Section 5

Proof of Lemma 5.2. Define permutations π_1, π_2 of $\mathbf{Z}_{m^{\alpha+1}}$ as follows. For each $a \in \mathbf{Z}_{m^{\alpha+1}}$, let $\sum_{i=0}^{\alpha} m^i a_i$ denote the base m representation of a . We define

$$\pi_1(a) = m^{\alpha} a_0 + \sum_{i=1}^{\alpha} m^{i-1} a_i \quad (102)$$

$$\pi_2(a) = a = \sum_{i=0}^{\alpha} m^i a_i. \quad (103)$$

The (non-linear) permutation π_1 performs a right-cyclic shift of the base- m digits of a , and π_2 is the identity permutation. For each $a \in \mathbf{Z}_{m^{\alpha+1}}$, we will show the mapping $a \mapsto (m\pi_1(a), sm^{\alpha}\pi_2(a))$ is injective. For each $a, b \in \mathbf{Z}_{m^{\alpha+1}}$, suppose

$$m\pi_1(a) = m\pi_1(b) \quad (\text{mod } m^{\alpha+1}) \quad (104)$$

$$sm^{\alpha}\pi_2(a) = sm^{\alpha}\pi_2(b) \quad (\text{mod } m^{\alpha+1}) \quad (105)$$

where $a = \sum_{i=0}^{\alpha} m^i a_i$ and $b = \sum_{i=0}^{\alpha} m^i b_i$. Then we have

$$\begin{aligned} \sum_{i=1}^{\alpha} m^i a_i &= \sum_{i=1}^{\alpha} m^i b_i & (\text{mod } m^{\alpha+1}) & \quad [\text{from (102), (104)}] \\ \therefore a_i &= b_i & (i = 1, 2, \dots, \alpha) & \quad [\text{from } 0 \leq a_i, b_i < m] \end{aligned}$$

and

$$\begin{aligned} sm^{\alpha} a_0 &= sm^{\alpha} b_0 & (\text{mod } m^{\alpha+1}) & \quad [\text{from (103), (105)}] \\ \therefore m^{\alpha} a_0 &= m^{\alpha} b_0 & (\text{mod } m^{\alpha+1}) & \quad [\text{from } \gcd(m, s) = 1] \\ \therefore a_0 &= b_0 & & \quad [\text{from } 0 \leq a_0, b_0 < m]. \end{aligned}$$

Thus $a = b$.

We have shown that $m\pi_1(a) = m\pi_1(b)$ and $sm^{\alpha}\pi_2(a) = sm^{\alpha}\pi_2(b)$ if and only if $a = b$. Thus a can be uniquely determined from $m\pi_1(a)$ and $sm^{\alpha}\pi_2(a)$. This implies the existence of the claimed mapping. ■

Proof of Lemma 5.4. Let π_1, π_2 and ψ be the permutations and mapping, respectively, from

Lemma 5.2. Define a code for the network $\mathcal{N}_3(m_1, m_2)$ over the ring $\mathbf{Z}_{m_1^{\alpha+1}}$, for each $l = 1, 2$, by:

$$\begin{aligned} e_0^{(l)} &= \sum_{j=1}^{m_l} x_j^{(l)} \\ e_i^{(l)} &= \pi_l(z) + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} x_j^{(l)} \quad (i = 1, 2, \dots, m_l) \\ e^{(l)} &= \pi_l(z) + \sum_{j=1}^{m_l} x_j^{(l)}. \end{aligned}$$

For each $l = 1, 2$, the receivers within the block $B^{(l)}(m_l)$ can recover their respective messages as follows:

$$\begin{aligned} R_0^{(l)} : \pi_l^{-1} \left(e^{(l)} - e_0^{(l)} \right) &= z \\ R_i^{(l)} : e^{(l)} - e_i^{(l)} &= x_i^{(l)} \quad (i = 1, 2, \dots, m_l). \end{aligned}$$

For each $l = 1, 2$, we have

$$\begin{aligned} -m_l e_0^{(l)} + \sum_{i=0}^{m_l} e_i^{(l)} &= -m_l \sum_{j=1}^{m_l} x_j^{(l)} + m_l \pi_l(z) + m_l \sum_{j=1}^{m_l} x_j^{(l)} \\ &= m_l \pi_l(z). \end{aligned} \tag{106}$$

The receiver R_z can recover z from its inputs as follows:

$$\begin{aligned} &\psi \left(-m_1 e_0^{(1)} + \sum_{i=0}^{m_1} e_i^{(1)}, -m_2 e_0^{(2)} + \sum_{i=0}^{m_2} e_i^{(2)} \right) \\ &= \psi (m_1 \pi_1(z), m_2 \pi_2(z)) \quad [\text{from (106)}] \\ &= \psi (m_1 \pi_1(z), sm_1^\alpha \pi_2(z)) = z \quad [\text{from } m_2 = sm_1^\alpha \text{ and Lemma 5.2}]. \end{aligned}$$

Thus the network code described above is, in fact, a solution for $\mathcal{N}_3(m_1, m_2)$. ■

Proof of Lemma 5.5. Assume $\mathcal{N}_3(m_1, m_2)$ is solvable over \mathcal{A} . For each $l = 1, 2$ the block $B^{(l)}(m_l)$ together with the source nodes $S_z, S_1^{(l)}, S_2^{(l)}, \dots, S_{m_l}^{(l)}$ forms a copy of $\mathcal{N}_0(m_l)$, so by Lemma 2.2, the edge functions within $B^{(1)}(m_1)$ and $B^{(2)}(m_2)$ must satisfy Property $P(m_1)$ and Property $P(m_2)$, respectively. Thus there exist Abelian groups (\mathcal{A}, \oplus_1) and (\mathcal{A}, \oplus_2) with identity elements 0_1 and 0_2 for the left-hand side and right-hand side of the network, respectively, and permutations $\pi_0^{(l)}, \pi_1^{(l)}, \dots, \pi_{m_l}^{(l)}$ and $\sigma_0^{(l)}, \sigma_1^{(l)}, \dots, \sigma_{m_l}^{(l)}$ of \mathcal{A} , such that for each $l = 1, 2$ the edges carry the

symbols:

$$e_0^{(l)} = \sigma_0^{(l)} \left(\bigoplus_{j=1}^{m_l} \pi_j^{(l)} \left(x_j^{(l)} \right) \right) \quad (107)$$

$$e_i^{(l)} = \sigma_i^{(l)} \left(\pi_0^{(l)}(z) \oplus_l \bigoplus_{\substack{j=1 \\ j \neq i}}^{m_l} \pi_j^{(l)} \left(x_j^{(l)} \right) \right) \quad (i = 1, 2, \dots, m_l) \quad (108)$$

$$e^{(l)} = \pi_0^{(l)}(z) \oplus_l \bigoplus_{j=1}^{m_l} \pi_j^{(l)} \left(x_j^{(l)} \right)$$

where \bigoplus in each of the previous three equations denotes \oplus_l .

Now suppose to the contrary that m_1 and $|\mathcal{A}|$ are not relatively prime and $|\mathcal{A}|$ divides m_2 . Then, since (\mathcal{A}, \oplus_2) is a finite group, for all $a \in \mathcal{A}$, we have

$$\underbrace{a \oplus_2 \cdots \oplus_2 a}_{m_2 \text{ adds}} = 0_2 \quad [\text{from } |\mathcal{A}| \mid m_2] . \quad (109)$$

Since m_1 and $|\mathcal{A}|$ are not relatively prime, m_1 and $|\mathcal{A}|$ share a common factor p . Since $p \mid |\mathcal{A}|$, by Cauchy's Theorem, there exists $a \in \mathcal{A} \setminus \{0_1\}$ such that the order of a is p , and since p divides m_1 we have $\underbrace{a \oplus_1 \cdots \oplus_1 a}_{m_1 \text{ adds}} = 0_1$. Define two collections of messages as follows:

$$\begin{aligned} x_j^{(1)} &= \pi_j^{(1)^{-1}}(0_1) & (j = 1, 2, \dots, m_1) \\ x_j^{(2)} &= \pi_j^{(2)^{-1}} \left(\pi_0^{(2)} \left(\pi_0^{(1)^{-1}}(0_1) \right) \right) & (j = 1, 2, \dots, m_2) \\ z &= \pi_0^{(1)^{-1}}(0_1) \end{aligned}$$

$$\begin{aligned} \hat{x}_j^{(1)} &= \pi_j^{(1)^{-1}}(a) & (j = 1, 2, \dots, m_1) \\ \hat{x}_j^{(2)} &= \pi_j^{(2)^{-1}} \left(\pi_0^{(2)} \left(\pi_0^{(1)^{-1}}(a) \right) \right) & (j = 1, 2, \dots, m_2) \\ \hat{z} &= \pi_0^{(1)^{-1}}(a). \end{aligned}$$

Since $a \neq 0_1$ and $\pi_0^{(1)}$ is bijective, it follows that $z \neq \hat{z}$. By Properties $P(m_1)$ and $P(m_2)$ and

(107) and (108), we have

$$\begin{aligned}
 e_i^{(1)} &= \sigma_i^{(1)} \left(\underbrace{0_1 \oplus_1 \cdots \oplus_1 0_1}_{m_1 \text{ adds}} \right) = \sigma_i^{(1)}(0_1) & (i = 0, 1, \dots, m_1) \\
 e_i^{(2)} &= \sigma_i^{(2)} \left(\underbrace{\pi_0^{(2)} \left(\pi_0^{(1)-1}(0_1) \right) \oplus_2 \cdots \oplus_2 \pi_0^{(2)} \left(\pi_0^{(1)-1}(0_1) \right)}_{m_2 \text{ adds}} \right) & (i = 0, 1, \dots, m_2) \\
 &= \sigma_i^{(2)}(0_2) & [\text{from (109)}]
 \end{aligned}$$

for the messages $x_j^{(l)}$, z , and

$$\begin{aligned}
 e_i^{(1)} &= \sigma_i^{(1)} \left(\underbrace{a \oplus_1 \cdots \oplus_1 a}_{m_1 \text{ adds}} \right) = \sigma_i^{(1)}(0_1) & (i = 0, 1, \dots, m_1) \\
 e_i^{(2)} &= \sigma_i^{(2)} \left(\underbrace{\pi_0^{(2)} \left(\pi_0^{(1)-1}(a) \right) \oplus_2 \cdots \oplus_2 \pi_0^{(2)} \left(\pi_0^{(1)-1}(a) \right)}_{m_2 \text{ adds}} \right) & (i = 0, 1, \dots, m_2) \\
 &= \sigma_i^{(2)}(0_2) & [\text{from (109)}]
 \end{aligned}$$

for the messages $\hat{x}_j^{(l)}$, \hat{z} . For both collections of messages, the edge symbols $e_0^{(1)}, e_1^{(1)}, \dots, e_{m_1}^{(1)}$ and $e_0^{(2)}, e_1^{(2)}, \dots, e_{m_2}^{(2)}$ are the same, and therefore the decoded value z at R_z must be the same. However, this contradicts the fact that $z \neq \hat{z}$. ■

Proof of Lemma 5.6. For any integers $a, b, c \geq 1$, we have $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$, so by Lemma 1.6 $\gcd(m_1, m_2)$ is invertible in R if and only if $\gcd(m_1, m_2, \text{char}(R)) = 1$. Thus it suffices to show that for each m_1, m_2 and each standard R -module G , network $\mathcal{N}_3(m_1, m_2)$ is scalar linear solvable over G if and only if $\gcd(m_1, m_2)$ is invertible in R .

Assume network $\mathcal{N}_3(m_1, m_2)$ is scalar linear solvable over standard R -module G . The messages are drawn from G , and there exist $c_{i,j}^{(l)}, c_j^{(l)} \in R$, such that for each $l = 1, 2$ the edge symbols can be written as:

$$e_0^{(l)} = \bigoplus_{j=1}^{m_l} \left(c_{0,j}^{(l)} \cdot x_j^{(l)} \right) \quad (110)$$

$$e_i^{(l)} = \left(c_{i,0}^{(l)} \cdot z \right) \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m_l} \left(c_{i,j}^{(l)} \cdot x_j^{(l)} \right) \quad (i = 1, \dots, m_l) \quad (111)$$

$$e^{(l)} = \left(c_0^{(l)} \cdot z \right) \oplus \bigoplus_{j=1}^{m_l} \left(c_j^{(l)} \cdot x_j^{(l)} \right) \quad (112)$$

and there exist $d_{i,e}^{(l)}, d_i^{(l)}, d_{z,i}^{(l)} \in R$, such that each receiver can linearly recover its respective message from its received edge symbols by:

$$R_0^{(l)} : z = \left(d_{0,e}^{(l)} \cdot e^{(l)} \right) \oplus \left(d_0^{(l)} \cdot e_0^{(l)} \right) \quad (l = 1, 2) \quad (113)$$

$$R_i^{(l)} : x_i^{(l)} = \left(d_{i,e}^{(l)} \cdot e^{(l)} \right) \oplus \left(d_i^{(l)} \cdot e_i^{(l)} \right) \quad \begin{matrix} (l = 1, 2) \\ (i = 1, \dots, m_l) \end{matrix} \quad (114)$$

$$R_z : z = \bigoplus_{l=1}^2 \bigoplus_{i=0}^{m_l} \left(d_{z,i}^{(l)} \cdot e_i^{(l)} \right). \quad (115)$$

For each $l = 1, 2$ the block $B^{(l)}(m_l)$ together with the source nodes $S_z, S_1^{(l)}, S_2^{(l)}, \dots, S_{m_l}^{(l)}$ forms a copy of $\mathcal{N}_0(m_l)$, so by Lemma 2.3 and (110) – (114), each $c_i^{(l)}$ and each $d_i^{(l)}$ is invertible in R , and

$$c_{i,j}^{(l)} = - \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_j^{(l)} \quad \begin{matrix} (l = 1, 2) \\ (i, j = 0, 1, \dots, m_l \text{ and } j \neq i). \end{matrix} \quad (116)$$

Equating message components at R_z yields:

$$\begin{aligned} 1_R &= \sum_{l=1}^2 \sum_{i=1}^{m_l} d_{z,i}^{(l)} c_{i,0}^{(l)} && [\text{from (110), (111), (115)}] \\ &= - \sum_{l=1}^2 \sum_{i=1}^{m_l} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_0^{(l)} && [\text{from (116)}] \end{aligned} \quad (117)$$

and for each $l = 1, 2$ we have

$$\begin{aligned} 0_R &= \sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} c_{i,j}^{(l)} && (j = 1, 2, \dots, m_l) \quad [\text{from (111), (110), (115)}] \\ &= - \left(\sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} \right) c_j^{(l)} && (j = 1, 2, \dots, m_l) \quad [\text{from (116)}]. \end{aligned} \quad (118)$$

For each $l = 1, 2$, by multiplying (118) by $\left(c_j^{(l)} \right)^{-1} c_0^{(l)}$, we have

$$0_R = \sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_0^{(l)} \quad (j = 1, 2, \dots, m_l). \quad (119)$$

Summing (119) over $l = 1, 2$ and $j = 1, 2, \dots, m_l$ and subtracting (117), yields

$$\begin{aligned} -1_R &= \sum_{l=1}^2 \sum_{j=0}^{m_l} \sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_0^{(l)} \\ &= \sum_{l=1}^2 m_l \sum_{i=0}^{m_l} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} c_0^{(l)}. \end{aligned} \quad (120)$$

Equation (120) implies there exist $r_1, r_2 \in R$ such that

$$1_R = m_1 r_1 + m_2 r_2. \quad (121)$$

Since $\gcd(m_1, m_2)$ can be factored out of both terms on the right-hand side of equation (121), the ring element $\gcd(m_1, m_2)$ is invertible.

To prove the converse, let G be a standard R -module, such that $\gcd(m_1, m_2)$ is invertible in R . Define a scalar linear code over G for $\mathcal{N}_3(m_1, m_2)$, for each $l = 1, 2$, by:

$$\begin{aligned} e_0^{(l)} &= \bigoplus_{j=1}^{m_l} x_j^{(l)} \\ e_i^{(l)} &= z \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m_l} x_j^{(l)} \quad (i = 1, \dots, m_l) \\ e^{(l)} &= z \oplus \bigoplus_{j=1}^{m_l} x_j^{(l)}. \end{aligned}$$

For each $l = 1, 2$, the receivers within $B^{(l)}(m_l)$ can linearly recover their respective messages by:

$$\begin{aligned} R_0^{(l)} : e^{(l)} \ominus e_0^{(l)} &= z \\ R_i^{(l)} : e^{(l)} \ominus e_i^{(l)} &= x_i^{(l)} \quad (i = 1, 2, \dots, m_l). \end{aligned}$$

Let $m'_1 = m_1/\gcd(m_1, m_2)$ and $m'_2 = m_2/\gcd(m_1, m_2)$. Then m'_1 and m'_2 are relatively prime, so there exist $n_1, n_2 \in \mathbf{Z}$ such that $n_1 m'_1 + n_2 m'_2 = 1$. Thus in R we have

$$(n_1 m'_1) 1_R + (n_2 m'_2) 1_R = 1_R.$$

Receiver R_z can linearly recover message z as follows:

$$\begin{aligned} R_z : & \bigoplus_{l=1}^2 \left((n_l \gcd(m_1, m_2)^{-1}) \cdot \left(\bigoplus_{i=0}^{m_l} e_i^{(l)} \ominus (m_l e_0^{(l)}) \right) \right) \\ &= \bigoplus_{l=1}^2 ((n_l \gcd(m_1, m_2)^{-1}) \cdot (m_l z)) \\ &= (n_1 m'_1 z) \oplus (n_2 m'_2 z) = ((n_1 m'_1) 1_R + (n_2 m'_2) 1_R) z = z. \end{aligned}$$

Thus the code is a scalar linear solution for $\mathcal{N}_3(m_1, m_2)$. ■

Proof of Lemma 5.8. By Lemma 5.6, network $\mathcal{N}_3(m_1, m_2)$ is scalar linear solvable over any finite-field alphabet whose characteristic is relatively prime to m_1 or m_2 , so the network's linear capacity for such finite-field alphabets is at least 1. By Lemma 2.4, network $\mathcal{N}_0(m_1)$ has capacity equal to 1, the block $B^{(1)}(m_1)$ together with the source nodes $S_z, S_1^{(1)}, S_2^{(1)}, \dots, S_{m_1}^{(1)}$ forms a copy of $\mathcal{N}_0(m_1)$, so the capacity of $\mathcal{N}_3(m_1, m_2)$ is at most 1. Thus both the capacity of $\mathcal{N}_3(m_1, m_2)$ and its linear capacity over any finite-field alphabet whose characteristic is relatively prime to m_1 or m_2 are 1.

To prove part (c), consider a (k, n) fractional linear solution for $\mathcal{N}_3(m_1, m_2)$ over a finite field \mathbb{F} whose characteristic divides both m_1 and m_2 . Since $\text{char}(\mathbb{F}) \mid m_1$ and $\text{char}(\mathbb{F}) \mid m_2$, we have $m_1 = m_2 = 0$ in \mathbb{F} .

We have $x_j^{(l)}, z \in \mathbb{F}^k$ and $e_i^{(l)}, e^{(l)} \in \mathbb{F}^n$, with $n \geq k$, since the capacity is one. There exist $n \times k$ coding matrices $M_j^{(l)}, M_{i,j}^{(l)}$ with entries in \mathbb{F} , such that for each $l = 1, 2$ the edge vectors can be written as:

$$e_0^{(l)} = \sum_{j=1}^{m_l} M_{0,j}^{(l)} x_j^{(l)} \tag{122}$$

$$e_i^{(l)} = M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_{i,j}^{(l)} x_j^{(l)} \quad (i = 1, 2, \dots, m_l) \tag{123}$$

$$e^{(l)} = M_0^{(l)} z + \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \tag{124}$$

and there exist $k \times n$ decoding matrices $D_{i,e}^{(l)}, D_i^{(l)}$ with entries in \mathbb{F} , such that for each $l = 1, 2$ the receivers within the block $B^{(l)}(m_l)$ can recover their respective messages from their received edge vectors by:

$$R_0^{(l)} : z = D_{0,e}^{(l)} e^{(l)} + D_0^{(l)} e_0^{(l)} \tag{125}$$

$$R_i^{(l)} : x_i^{(l)} = D_{i,e}^{(l)} e^{(l)} + D_i^{(l)} e_i^{(l)} \quad (i = 1, 2, \dots, m_l). \tag{126}$$

Since the receiver R_z recovers message z linearly from its incoming edge vectors, we have

$$\left\{ e_i^{(l)} : \begin{array}{l} l = 1, 2 \\ i = 0, 1, \dots, m_l \end{array} \right\} \longrightarrow z. \quad (127)$$

By setting $z = 0$ in (125), for each $l = 1, 2$ we have

$$\begin{aligned} 0 &= D_{0,e}^{(l)} \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} + D_0^{(l)} e_0^{(l)} && [\text{from (122), (124), (125)}] \\ \therefore \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} &\longrightarrow D_0^{(l)} e_0^{(l)}, && (128) \end{aligned}$$

and similarly, by setting $x_i^{(l)} = 0$ in (126) for $l = 1, 2$ we have

$$\begin{aligned} 0 &= D_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \right) + D_i^{(l)} e_i^{(l)} \quad (i = 1, 2, \dots, m_l) && [\text{from (123), (124), (125)}] \\ \therefore e_i^{(l)} &\longrightarrow D_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \right) && (i = 1, 2, \dots, m_l). \end{aligned} \quad (129)$$

As in Lemma 3.8, for each $l = 1, 2$ and $i = 1, 2, \dots, m_l$, let $Q_0^{(l)}$ be the matrix Q in Lemma 3.7 corresponding to when $D_0^{(l)}$ is the matrix A in the lemma, and let $Q_{i,e}^{(l)}$ be the matrix Q corresponding to when $D_{i,e}^{(l)}$ is the matrix A .

Let $L^{(1)}$ and $L^{(2)}$ be the lists from Lemma 3.8 (where z plays the role of x_0), corresponding to the left-hand side and right-hand side of the network, respectively. Specifically, for each $l = 1, 2$, let $L^{(l)}$ be the list

$$\begin{aligned} &Q_0^{(l)} e_0^{(l)} \\ &e_i^{(l)} && (i = 1, 2, \dots, m_l) \\ &Q_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \right) && (i = 1, 2, \dots, m_l). \end{aligned}$$

For each $l = 1, 2$ we have

$$L^{(l)} \longrightarrow D_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \right) \quad [\text{from (129)}] \quad (130)$$

$$L^{(l)} \longrightarrow M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \quad [\text{from Lemma 3.7, (130)}] . \quad (131)$$

For each $l = 1, 2$ we also have

$$\begin{aligned} & \left\{ M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} : i = 1, 2, \dots, m_l \right\} \\ & \longrightarrow \sum_{i=1}^{m_l} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \right) \\ & = m_l M_0^{(l)} z + (m_l - 1) \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \\ & = - \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \quad [\text{from } \text{char}(\mathbb{F}) \mid m_l] , \end{aligned} \quad (132)$$

and so

$$L^{(l)} \longrightarrow \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \quad [\text{from (132), (131)}] \quad (133)$$

$$L^{(l)} \longrightarrow D_0^{(l)} e_0^{(l)} \quad [\text{from (128), (133)}] \quad (134)$$

$$L^{(l)} \longrightarrow e_0^{(l)} \quad [\text{from Lemma 3.7, (134)}] . \quad (135)$$

We have

$$L^{(1)}, L^{(2)} \longrightarrow z \quad [\text{from (127), (135)}] . \quad (136)$$

For each $l = 1, 2$ we also have

$$z, \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \longrightarrow e^{(l)} \quad [\text{from (124)}] \quad (137)$$

$$L^{(l)}, z \longrightarrow e^{(l)} \quad [\text{from (133), (137)}] \quad (138)$$

$$L^{(l)}, z \longrightarrow x_i^{(l)} \quad (i = 1, 2, \dots, m_l) \quad [\text{from (126), (138)}]. \quad (139)$$

Thus

$$L^{(1)}, L^{(2)} \longrightarrow z, \left\{ x_i^{(l)} : \begin{array}{l} l = 1, 2 \\ i = 1, 2, \dots, m_l \end{array} \right\} \quad [\text{from (136), (139)}]. \quad (140)$$

We have $L^{(l)}$ corresponding to the same set of vector functions as the list L for $\mathcal{N}_1(m_l)$ in Lemma 3.8 (with a slight change of labeling). Thus the bound on the entropy of the list L in (61) in Lemma 3.8 can be used to bound the entropy of the list $L^{(1)}, L^{(2)}$:

$$H(L^{(1)}, L^{(2)}) \leq (2m_1 + 2m_2 + 2)n - (m_1 + m_2 + 2)k \quad [\text{from (61)}]. \quad (141)$$

But then we have

$$\begin{aligned} (m_1 + m_2 + 1)k &= H\left(z, \left\{ x_i^{(l)} : \begin{array}{l} l = 1, 2 \\ i = 1, 2, \dots, m_l \end{array} \right\}\right) && [\text{from } z, x_i^{(l)} \in \mathbb{F}^k] \\ &\leq H(L_1, L_2) && [\text{from (140)}] \\ &\leq (2m_1 + 2m_2 + 2)n - (m_1 + m_2 + 2)k && [\text{from (141)}] \\ \therefore \frac{k}{n} &\leq \frac{2m_1 + 2m_2 + 2}{2m_1 + 2m_2 + 3}. \end{aligned}$$

Thus the linear capacity of $\mathcal{N}_3(m_1, m_2)$ for finite-field alphabets whose characteristic divides both m_1 and m_2 is upper bounded by

$$1 - \frac{1}{2m_1 + 2m_2 + 3}.$$

Consider a $(2m_1 + 2m_2 + 2, 2m_1 + 2m_2 + 3)$ fractional linear code for $\mathcal{N}_3(m_1, m_2)$ over any finite-field alphabet whose characteristic divides both m_1 and m_2 , described below.

The edges symbols on the left-hand side of $\mathcal{N}_3(m_1, m_2)$ are given by:

$$\begin{aligned}
 [e_0^{(1)}]_l &= \begin{cases} \sum_{\substack{j=1 \\ j \neq l}}^{m_1} [x_j^{(1)}]_l & (l = 1, 2, \dots, m_1) \\ \sum_{j=1}^{m_1} [x_j^{(1)}]_l & (l = m_1 + 1, \dots, 2m_1 + 2m_2 + 2) \\ \sum_{j=2}^{m_1} [x_j^{(1)}]_j & (l = 2m_1 + 2m_2 + 3) \end{cases} \\
 [e_i^{(1)}]_l &= \begin{cases} [z]_l + \sum_{\substack{j=1 \\ j \neq i \\ j \neq l}}^{m_1} [x_j^{(1)}]_l & (l = 1, 2, \dots, m_1 \text{ and } l \neq i) \\ [z]_{m_1+1} + \sum_{\substack{j=1 \\ j \neq i}}^{m_1} [x_j^{(1)}]_j & (l = i) \\ [z]_l + \sum_{\substack{j=1 \\ j \neq i}}^{m_1} [x_j^{(1)}]_l & (l = m_1 + 1, \dots, 2m_1 + 2m_2 + 2) \\ [z]_{m_1+i+1} & (l = 2m_1 + 2m_2 + 3) \end{cases} \quad (i = 1, 2, \dots, m_1) \\
 [e^{(1)}]_l &= \begin{cases} [z]_l + \sum_{\substack{j=1 \\ j \neq l}}^{m_1} [x_j^{(1)}]_l & (l = 1, 2, \dots, m_1) \\ [z]_l + \sum_{j=1}^{m_1} [x_j^{(1)}]_l & (l = m_1 + 1, \dots, 2m_1 + 2m_2 + 2) \\ [z]_{m_1+1} + \sum_{j=1}^{m_1} [x_j^{(1)}]_j & (l = 2m_1 + 2m_2 + 3). \end{cases}
 \end{aligned}$$

For brevity, let $\delta = 2m_1 + m_2 + 2 = n - (m_2 + 1)$. The edges symbols on the right-hand side of $\mathcal{N}_3(m_1, m_2)$ are given by:

$$\begin{aligned}
 [e_0^{(2)}]_l &= \begin{cases} \sum_{j=1}^{m_2} [x_j^{(2)}]_l & (l = 1, 2, \dots, \delta) \\ \sum_{\substack{j=1 \\ j \neq l-\delta}}^{m_2} [x_j^{(2)}]_l & (l = \delta + 1, \dots, \delta + m_2) \\ \sum_{j=2}^{m_2} [x_j^{(2)}]_{\delta+j} & (l = \delta + m_2 + 1) \end{cases} \\
 [e_i^{(2)}]_l &= \begin{cases} [z]_l + \sum_{\substack{j=1 \\ j \neq i}}^{m_2} [x_j^{(2)}]_l & (l = 1, 2, \dots, \delta) \\ [z]_\delta + \sum_{\substack{j=1 \\ j \neq i}}^{m_2} [x_j^{(2)}]_{\delta+j} & (l = \delta + i) \\ [z]_l + \sum_{\substack{j=1 \\ j \neq i \\ j \neq l-\delta}}^{m_2} [x_j^{(2)}]_l & \left(\begin{array}{l} l = \delta + 1, \dots, \delta + m_2 \\ \text{and } l \neq \delta + i \end{array} \right) \\ [z]_{2m_1+1+i} & (l = \delta + m_2 + 1) \end{cases} \quad (i = 1, 2, \dots, m_2) \\
 [e^{(2)}]_l &= \begin{cases} [z]_l + \sum_{j=1}^{m_2} [x_j^{(2)}]_l & (l = 1, 2, \dots, \delta) \\ [z]_l + \sum_{\substack{j=1 \\ j \neq l-\delta}}^{m_2} [x_j^{(2)}]_l & (l = \delta + 1, \dots, \delta + m_2) \\ [z]_\delta + \sum_{j=1}^{m_2} [x_j^{(2)}]_{\delta+j} & (l = \delta + m_2 + 1). \end{cases}
 \end{aligned}$$

We have

$$\begin{aligned} \sum_{\substack{i=1 \\ i \neq l}}^{m_1} [e_i^{(1)}]_l &= (m_1 - 1) [z]_l + (m_1 - 2) \sum_{\substack{j=1 \\ j \neq l}}^{m_1} [x_j^{(1)}]_l & (l = 1, 2, \dots, m_1) \\ &= -[z]_l - 2 [e_0^{(1)}]_l & [\text{from char}(\mathbb{F}) \mid m_1] \end{aligned} \quad (142)$$

$$\begin{aligned} \sum_{\substack{i=1 \\ i \neq l-\delta}}^{m_2} [e_i^{(2)}]_l &= (m_2 - 1) [z]_l + (m_2 - 2) \sum_{\substack{j=1 \\ j \neq l-\delta}}^{m_2} [x_j^{(2)}]_l & (l = \delta + 1, \dots, \delta + m_2) \\ &= -[z]_l - 2 [e_0^{(2)}]_l & [\text{from char}(\mathbb{F}) \mid m_2]. \end{aligned} \quad (143)$$

Each of the receivers can linearly recover each of the $2m_1 + 2m_2 + 2$ components of its demanded message from its received vectors by:

$$R_0^{(1)} : [e^{(1)}]_l - [e_0^{(1)}]_l = [z]_l \quad (l = 1, 2, \dots, 2m_1 + 2m_2 + 2)$$

$$\begin{aligned} R_i^{(1)} : [e^{(1)}]_{2m_1+2m_2+3} - [e_i^{(1)}]_i &= [x_i^{(1)}]_i & (i = 1, 2, \dots, m_1) \\ [e^{(1)}]_l - [e_i^{(1)}]_l &= [x_i^{(1)}]_l & (l = 1, 2, \dots, 2m_1 + 2m_2 + 2 \text{ and } l \neq i) \end{aligned}$$

$$R_0^{(2)} : [e^{(2)}]_l - [e_0^{(2)}]_l = [z]_l \quad (l = 1, 2, \dots, 2m_1 + 2m_2 + 2)$$

$$\begin{aligned} R_i^{(2)} : [e^{(2)}]_{\delta+m_2+1} - [e_i^{(2)}]_{\delta+i} &= [x_i^{(2)}]_{\delta+i} & (i = 1, 2, \dots, m_2) \\ [e^{(2)}]_l - [e_i^{(2)}]_l &= [x_i^{(2)}]_l & (l = 1, 2, \dots, 2m_1 + 2m_2 + 2 \text{ and } l \neq \delta + i) \end{aligned}$$

$$R_z : \quad -2 \left[e_0^{(1)} \right]_l - \sum_{\substack{i=1 \\ i \neq l}}^{m_1} \left[e_i^{(1)} \right]_l = [z]_l \quad (l = 1, 2, \dots, m_1) \quad [\text{from (142)}]$$

$$\left[e_1^{(1)} \right]_1 - \left[e_0^{(1)} \right]_{2m_1+2m_2+3} = [z]_{m_1+1}$$

$$\left[e_{l-m_1-1}^{(1)} \right]_{2m_1+2m_2+3} = [z]_l \quad (l = m_1 + 2, \dots, 2m_1 + 1)$$

$$\left[e_{l-2m_1-1}^{(2)} \right]_{\delta+m_1+1} = [z]_l \quad (l = 2m_1 + 2, \dots, 2m_1 + m_2 + 1)$$

$$\left[e_1^{(2)} \right]_{\delta+1} - \left[e_0^{(2)} \right]_{2_1+2m_2+3} = [z]_\delta \quad (\delta = 2m_1 + m_2 + 2)$$

$$-2 \left[e_0^{(2)} \right]_l - \sum_{\substack{i=1 \\ i \neq l-\delta}}^{m_2} \left[e_i^{(2)} \right]_l = [z]_l \quad (l = \delta + 1, \dots, \delta + m_2) \quad [\text{from (143)}].$$

Thus the code is in fact a linear solution for $\mathcal{N}_3(m_1, m_2)$. ■

References

- [1] R. Ahlswede, C. Ning, S.-Y.R. Li, R.W. Yeung, “Network information flow,” *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.
- [2] A. Blasiak, R. Kleinberg, and E. Lubetzky, “Lexicographic products and the power of non-linear network coding,” *IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 609–618, October 2011.
- [3] K. Cai and G. Han, “On the solvability of three-pair networks with common bottleneck links,” *IEEE Information Theory Workshop (ITW)*, pp. 546–550, November 2–5, 2014.
- [4] J. Cannons, R. Dougherty, C. Freiling, and K. Zeger, “Network routing capacity,” *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 777–788, March 2006.
- [5] T. Chan and A. Grant, “Dualities between entropy functions and network codes,” *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4470–4487, October 2008.
- [6] Y. Chen and K. HaiBin, “A characterization of solvability for a class of networks” *Science China Information Sciences*, vol. 55, no. 4, pp. 747–754, April 2012.
- [7] R. Dougherty, C. Freiling, and K. Zeger, “Insufficiency of linear coding in network information flow,” *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2745–2759, August 2005.
- [8] R. Dougherty, C. Freiling, K. Zeger, “Linear network codes and systems of polynomial equations,” *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2303–2316, May 2008.
- [9] R. Dougherty, C. Freiling, and K. Zeger, “Linearity and solvability in multicast networks,” *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2243–2256, October 2004.
- [10] R. Dougherty, C. Freiling, and K. Zeger, “Networks, matroids, and non-Shannon information inequalities,” *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 1949–1969, June 2007.
- [11] R. Dougherty, C. Freiling, and K. Zeger, “Unachievability of network coding capacity,” *IEEE Transactions on Information Theory (joint issue with IEEE/ACM Transactions on Networking)*, vol. 52, no. 6, pp. 2365–2372, June 2006.
- [12] D. Dummit and R. Foote, *Abstract Algebra*, Third Edition, Hoboken, NJ, John Wiley and Sons Inc., 2004.
- [13] S. El Rouayheb, A. Sprintson, and C. Georgiades, “On the index coding problem and its relation to network coding and matroid theory,” *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3187–3195, July 2010.
- [14] M. Feder, D. Ron, and A. Tavor, “Bounds on linear codes for network multicast,” *Electronic Colloquium on Computational Complexity (ECCC)*, pp. 1–9, 2003.

- [15] R. Koetter and M. Médard, “An algebraic approach to network coding,” *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, October 2003.
- [16] R. Koetter, Keynote presentation at *International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt 2008)*, March 31 – April 4, 2008, Berlin, Germany,
http://www.wiopt.org/wiopt08/pdf/talk_Koetter_WiOpt08.pdf.
- [17] P. Krishnan and B.S. Rajan, “A matroidal framework for network-error correcting codes,” *IEEE Transactions on Information Theory*, vol. 61, no. 2, pp. 836–872, February 2015.
- [18] F. Kschischang, “An Introduction to Network Coding,” chapter 1 in: *Network Coding: Fundamentals and Applications*, M. Médard and A. Sprintson, editors, Academic Press, 2012.
- [19] S.-Y.R. Li, R.W. Yeung, C. Ning, “Linear network coding,” *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, February 2003.
- [20] M. Médard, M. Effros, T. Ho, and D. Karger, “On coding for non-multicast networks,” *Conference on Communication Control and Computing*, Monticello, IL, October 2003.
- [21] B.K. Rai and B.K. Dey, “On network coding for sum-networks,” *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 50–63, January 2012.
- [22] A. Rasala Lehman and E. Lehman, “Complexity classification of network information flow problems,” *ACM-SIAM Symposium on Discrete algorithms*, 2004.
- [23] S. Riis, “Linear versus nonlinear boolean functions in network flow,” *Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March 2004.
- [24] G. Robin, “Estimation de la fonction de Tchebychef θ sur le k -ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n ” (in French), *Acta Arithmetica*, vol. 42, no. 4, pp. 367–389, 1983.
- [25] J. Sándor, D.S. Mitrinovic, and B. Crstici, *Handbook of Number Theory I*, Springer, 2006.
- [26] I. Satake, *Linear Algebra*. New York: Marcel Dekker, 1975.
- [27] S. Shenvi and B.K. Dey, “A simple necessary and sufficient condition for the double unicast problem,” *IEEE International Conference on Communications (ICC)*, pp. 1–5, May 2010.
- [28] A. T. Subramanian and A. Thangaraj, “Path gain algebraic formulation for the scalar linear network coding problem,” *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4520–4531, September 2010.
- [29] Q. Sun, X. Yin, Z. Li, K. Long, “Multicast network coding and field sizes,” *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6182–6191, November 2015.